#### (19) 世界知的所有権機関 国際事務局



## 

#### (43) 国際公開日 2001年1月11日(11.01.2001)

#### PCT

# (10) 国際公開番号

WO 01/02968 A1

(51) 国際特許分類?: 9/08, 9/32, G10K 15/02, G06F 13/00

G06F 15/00, 17/60, H04L

特願2000/126305

2000年4月21日(21.04.2000)

JP

(21) 国際出願番号:

PCT/JP00/04488

(71) 出願人 (米国を除く全ての指定国について): ソニー株 式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001

(22) 国際出願日:

2000年7月6日(06.07.2000)

(72) 発明者; および

(25) 国際出願の言語:

日本語

(75) 発明者/出願人 (米国についてのみ): 野中 聡 (NON-AKA, Akira) [JP/JP]. 江崎 正 (EZAKI, Tadashi)

[JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35

号 ソニー株式会社内 Tokyo (JP).

(26) 国際公開の言語:

日本語

JP

(30) 優先権データ:

特願平11/192413 特願平11/193561 1999年7月6日 (06.07.1999) JP 1999 年7 月7 日 (07.07.1999) JP

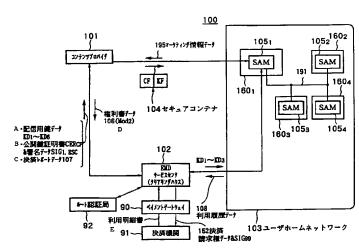
特願平11/193562 1999 年7 月7 日 (07.07.1999) (74) 代理人: 佐藤隆久(SATOH, Takahisa); 〒111-0052 東 京都台東区柳橋2丁目4番2号 宮木ビル4階 創進国際 特許事務所 Tokyo (JP).

東京都品川区北品川6丁目7番35号 Tokyo (JP).

/続葉有/

(54) Title: DATA PROVIDING SYSTEM, DEVICE, AND METHOD

(54) 発明の名称: データ提供システム、装置およびその方法



(57) Abstract: A content provider (101) distributes a secure container (104) containing content data encrypted with a content key data, content key data encrypted with distribution key data, and title deed data encrypted and representing the handling of the content data to, e.g., an SAM (105<sub>1</sub>) of a user home network (103). The SAM (105<sub>1</sub>) decodes the content key data and title deed data contained in the secure container (104), and determines the handling including the form of purchase and the form of the use of the content data according to the decrypted title deed data.

A...DISTRIBUTION KEY DATA KD1 TO KD6

B...PUBLIC KEY CERTIFICATION CERCP & SIGNATURE DATA SIG1, ESC

C...SETTELEMENT REPORT DATA 107

101...CONTENT PROVIDER

D...TITLE DEED DATA 106 (Mod2)

195...MARKETING INFORMATION DATA

104...SECURE CONTAINER

92...ROUTE AUTHENTICATION AGENCY

102...EMD SERVICE CENTER (CLEARING HOUCE)

90...PAYMENT GATEWAY

E...USE SPECIFICATIONS

91...SETTLEMENT INSTITUTION

108...USE HISTORY DATA

152...SETTLEMENT CLAIM DATA & SIG99

103...USER HOME NETWORK





- (81) 指定国 (国内): CN, KR, US.
- (84) 指定国 *(*広域*)*: ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

#### 添付公開書類:

- -- 国際調査報告書
- 請求の範囲の補正の期限前の公開であり、補正書受領の際には再公開される。

(57) 要約:

コンテンツプロバイダ101は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、配信鍵用データを用いて暗号化されたコンテンツ鍵データと、コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したセキュアコンテナ104をユーザホームネットワーク103のSAM105」などに配給する。SAM105」などは、セキュアコンテナ104に格納されたコンテンツ鍵データおよび権利書データを復号し、当該復号した権利書データに基づいて、コンテンツデータの購入形態および利用形態などの取り扱いを決定する。

#### 明細書

## データ提供システム、装置およびその方法

#### 技術分野

本発明は、コンテンツデータを提供するデータ提供システム、データ提供装置 およびそれらの方法と、これらに用いられる管理装置およびデータ処理装置に関 する。

#### 背景技術

暗号化されたコンテンツデータを所定の契約を交わしたユーザのデータ処理装 置に配給し、当該データ処理装置において、コンテンツデータを復号して再生お よび記録するデータ提供システムがある。

このようなデータ提供システムの一つに、音楽データを配信する従来のEMD (Electronic Music Distribution: 電子音楽配信)システムがある。

図100は、従来のEMDシステム700の構成図である。

図100に示すEMDシステム700では、コンテンツプロバイダ701a, 701bが、サービスプロバイダ710に対し、コンテンツデータ704a,7 04b, 704cと、著作権情報705a, 705b, 705cとを、それぞれ 相互認証後に得たセッション鍵データで暗号化してオンラインで供給したり、あ るいはオフラインで供給する。ここで、著作権情報705g,705b,705 cには、例えば、SCMS(Serial Copy Management System) 情報、コンテンツ データに埋め込むことを要請する電子透かし情報およびサービスプロバイダ71 0の伝送プロトコルに埋め込むことを要請する著作権に関する情報などがある。 サービスプロバイダ710は、受信したコンテンツデータ704a,704b

, 704 cと、著作権情報 705 a, 705 b, 705 cとをセッション鍵デー

夕を用いて復号する。

そして、サービスプロバイダ710は、復号したあるいはオフラインで受け取ったコンテンツデータ704a,704b,704cに、著作権情報705a,705b,705cを埋め込んで、コンテンツデータ707a,707b,707cを生成する。このとき、サービスプロバイダ710は、例えば、著作権情報705a,705b,705cのうち電子透かし情報をコンテンツデータ704a,704b,704cに所定の周波数領域を変更して埋め込み、当該コンテンツデータをユーザに送信する際に用いるネットワークプロトコルにSCMS情報を埋め込む。

さらに、サービスプロバイダ710は、コンテンツデータ707a,707b,707cを、鍵データベース706から読み出したコンテンツ鍵データKca,Kcb,Kccを用いてそれぞれ暗号化する。その後、サービスプロバイダ710は、暗号化されたコンテンツデータ707a,707b,707cを格納したセキュアコンテナ722を、相互認証後に得たセッション鍵データによって暗号化してユーザの端末装置709に存在するCA(Conditional Access)モジュール711に送信する。

CAモジュール711は、セキュアコンテナ722をセッション鍵データを用いて復号する。また、CAモジュール711は、電子決済やCAなどの課金機能を用いて、サービスプロバイダ710の鍵データベース706からコンテンツ鍵データKca,Kcb,Kccを受信し、これをセッション鍵データを用いて復号する。これにより、端末装置709において、コンテンツデータ707a,707b,707cを、それぞれコンテンツ鍵データKca,Kcb,Kccを用いて復号することが可能になる。

このとき、CAモジュール711は、コンテンツ単位で課金処理を行い、その 結果に応じた課金情報721を生成し、これをセッション鍵データで暗号化した 後に、サービスプロバイダ710の権利処理モジュール720に送信する。

この場合に、CAモジュール711は、サービスプロバイダ710が自らの提供するサービスに関して管理したい項目であるユーザの契約(更新)情報および 月々基本料金などのネットワーク家賃の徴収と、コンテンツ単位の課金処理と、 ネットワークの物理層のセキュリティー確保とを行う。

サービスプロバイダ710は、CAモジュール711から課金情報721を受信すると、サービスプロバイダ710とコンテンツプロバイダ701a,701 b,701cとの間で利益配分を行う。

このとき、サービスプロバイダ710から、コンテンツプロバイダ701a,701b,701cへの利益配分は、例えば、JASRAC(Japanese Society for Rights of Authors, Composers and Publishers:日本音楽著作権協会)を介して行われる。また、JASRACによって、コンテンツプロバイダの利益が、当該コンテンツデータの著作権者、アーティスト、作詞・作曲家および所属プロダクションなどに分配される。

また、端末装置709では、コンテンツ鍵データKca,Kcb,Kccを用いて復号したコンテンツデータ707a,707b,707cを、RAM型の記録媒体723などに記録する際に、著作権情報705a,705b,705cのSCMSビットを書き換えて、コピー制御を行う。すなわち、ユーザ側では、コンテンツデータ707a,707b,707cに埋め込まれたSCMSビットに基づいて、コピー制御が行われ、著作権の保護が図られている。

ところで、SCMSは、CD(Compact Disc)からDAT(Digital Audio Tape) への録音を防止するために規定されたものであり、DATとDATとの間での複製が可能である。また、コンテンツデータに電子透かし情報を埋め込んだ場合も、問題が生じたときに、対象となっているコンテンツデータを提供したコンテンツプロバイダを特定するに止まり、違法なコピーを技術的に阻止するものではない。

従って、上述した図100に示すEMDシステム700では、コンテンツプロ

バイダの権利(利益)が十分に保護されないという問題がある。

また、上述したEMDシステム700では、コンテンツプロバイダの著作権情報をサービスプロバイダがコンテンツデータに埋め込むため、コンテンツプロバイダは当該埋め込みが要求通りに行われているかを監査する必要がある。また、コンテンツプロバイダは、サービスプロバイダが契約通りに、コンテンツデータの配信を行っているかを監査する必要がある。そのため、監査のための負担が大きいという問題がある。

また、上述したEMDシステム700では、ユーザの端末装置709からの課金情報721を、サービスプロバイダ710の権利処理モジュール720で処理するため、ユーザによるコンテンツデータの利用に応じてコンテンツプロバイダが受けるべき利益を、コンテンツプロバイダが適切に受けられるかどうかが懸念される。

## 発明の開示

本発明は上述した従来技術の問題点に鑑みてなされ、コンテンプロバイダの権利者(関係者)の利益を適切に保護できるデータ提供システム、データ提供装置およびそれらの方法とデータ処理装置と管理装置とを提供することを目的とする

また、本発明は、コンテンプロバイダの権利者の利益を保護するための監査の 負担を軽減できるデータ提供システム、データ提供装置およびそれらの方法とデ ータ処理装置と管理装置とを提供することを目的とする。

上述した従来技術の問題点を解決し、上述した目的を達成するために、第1の 発明のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツ データを配給するデータ提供システムであって、前記データ提供装置は、コンテ ンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コン テンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書

データとを格納したモジュールを前記データ処理装置に配給し、前記データ処理 装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データ および前記権利書データを復号し、当該復号した権利書データに基づいて、前記 コンテンツデータの取り扱いを決定する。

第1の発明のデータ提供システムでは、前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールが配給される。

そして、前記データ処理装置において、前記配給を受けた前記モジュールに格 納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号し た権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

このように、コンテンツデータを格納したモジュールに、当該コンテンツデータの取り扱いを示す権利書データを格納することで、データ処理装置において、データ提供装置の関係者が作成した権利書データに基づいたコンテンツデータの取り扱い(利用)を行わせることが可能になる。

また、第1の発明のデータ提供システムは、好ましくは、前記データ提供装置は、配信用鍵データを用いてそれぞれ暗号化された前記コンテンツ鍵データおよび前記権利書データを格納した前記モジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを前記配信用鍵データを用いて復号する

また、第1の発明のデータ提供システムは、好ましくは、前記配信用鍵データを管理し、前記データ提供装置および前記データ処理装置に前記配信用鍵データを配給する管理装置をさらに有する。

また、第2の発明のデータ処理装置は、データ提供装置から配給されたコンテ ンツデータを利用するデータ処理装置であって、コンテンツ鍵データを用いて暗

ο.

号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを前記データ提供装置から受けて、当該受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、第3の発明のデータ提供システムは、データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

第3の発明のデータ提供システムでは、前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールが提供される。

次に、前記データ配給装置から前記データ処理装置に、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールが配給される。

次に、前記データ処理装置において、前記配給を受けた前記第2のモジュール に格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該 復号した権利書データに基づいて、前記コンテンツデータの取り扱いが決定され

る。

また、第3の発明のデータ提供システムは、好ましくは、前記データ配給装置は、前記コンテンツデータの価格を示す価格データを格納した前記第2のモジュールを前記データ処理装置に配給する。

また、第4の発明のデータ提供システムは、データ提供装置と、少なくとも第1のデータ配給装置および第2のデータ配給装置と、データ処理装置とを有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記複数のデータ配給装置に提供し、前記第1のデータ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを前記データ処理装置に配給し、前記第2のデータ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第3のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第2のモジュールおよび前記第3のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、第5の発明のデータ提供システムは、少なくとも第1のデータ提供装置および第2のデータ提供装置と、データ配給装置と、データ処理装置とを有するデータ提供システムであって、前記第1のデータ提供装置は、第1のコンテンツ鍵データを用いて暗号化された第1のコンテンツデータと、暗号化された前記第1のコンテンツ鍵データと、前記第1のコンテンツデータの取り扱いを示す暗号化された第1の権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、前記第2のデータ提供装置は、第2のコンテンツ鍵データを用いて

暗号化された第2のコンテンツデータと、暗号化された前記第2のコンテンツ鍵データと、前記第2のコンテンツデータの取り扱いを示す暗号化された第2の権利書データとを格納した第2のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化された前記第1のコンテンツデータ、前記第1のコンテンツ鍵データおよび前記第1の権利書データと、前記提供を受けた前記第2のコンテンツ鍵データおよび前記第2のコンテンツデータ、前記第2のコンテンツ鍵データおよび前記第2の相利書データとを格納した第3のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第3のモジュールに格納された前記第1のコンテンツ鍵データおよび前記第1の福利書データを復号し、当該復号した第1の権利書データに基づいて、前記第1のコンテンツデータの取り扱いを決定し、前記配給を受けた前記第3のモジュールに格納された前記第2のコンテンツ鍵データおよび前記第2の福利書データを復号し、当該復号した第2の権利書データに基づいて、前記第2のコンテンツデータの取り扱いを決定する。

また、第6の発明のデータ提供装置は、コンテンツデータの利用を行うデータ処理装置に、前記コンテンツデータを配給するデータ提供装置であって、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを前記データ処理装置に配給する。

また、第7の発明のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供方法であって、前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを配給し、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コン

テンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに 基づいて、前記コンテンツデータの取り扱いを決定する。

また、第8の発明のデータ提供方法は、データ提供装置、データ配給装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを提供し、前記データ配給装置から前記データ処理装置に、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを配給し、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、第9の発明のデータ提供方法は、データ提供装置と、少なくとも第1のデータ配給装置および第2のデータ配給装置と、データ処理装置とを用いたデータ提供方法であって、前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを提供し、前記第1のデータ配給装置から前記データ処理装置に、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを配給し、前記第2のデータ配給装置から前記データ処理装置に、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第3のモジュールを配給し、前記データ処理装置において、前記配給を受けた前記第2のモジュールおよび前記第3のモジュールに格納された前記コンテンツ鍵データお

よび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、第10の発明のデータ提供方法は、少なくとも第1のデータ提供装置お よび第2のデータ提供装置と、データ配給装置と、データ処理装置とを用いたデ ータ提供方法であって、前記第1のデータ提供装置から前記データ配給装置に、 第1のコンテンツ鍵データを用いて暗号化された第1のコンテンツデータと、暗 号化された前記第1のコンテンツ鍵データと、前記第1のコンテンツデータの取 り扱いを示す暗号化された第1の権利書データとを格納した第1のモジュールを 提供し、前記第2のデータ提供装置から前記データ配給装置に、第2のコンテン ツ鍵データを用いて暗号化された第2のコンテンツデータと、暗号化された前記 第2のコンテンツ鍵データと、前記第2のコンテンツデータの取り扱いを示す暗 号化された第2の権利書データとを格納した第2のモジュールを提供し、前記デ ータ配給装置から前記データ処理装置に、前記提供を受けた前記第1のモジュー ルに格納された前記暗号化された前記第1のコンテンツデータ、前記第1のコン テンツ鍵データおよび前記第1の権利書データと、前記提供を受けた前記第2の モジュールに格納された前記暗号化された前記第2のコンテンツデータ、前記第 2のコンテンツ鍵データおよび前記第2の権利書データとを格納した第3のモジ ュールを配給し、前記データ処理装置において、前記配給を受けた前記第3のモ ジュールに格納された前記第1のコンテンツ鍵データおよび前記第1の権利書デ ータを復号し、当該復号した第1の権利書データに基づいて、前記第1のコンテ ンツデータの取り扱いを決定し、前記配給を受けた前記第3のモジュールに格納 された前記第2のコンテンツ鍵データおよび前記第2の権利書データを復号し、 当該復号した第2の権利書データに基づいて、前記第2のコンテンツデータの取 り扱いを決定する。

また、第11の発明のデータ提供システムは、データ提供装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は

、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ処理装置に配給し、前記権利書データの正当性を証明することを前記管理装置に要求し、前記データ処理装置は、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行い、前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、前記データ提供装置からの要求に応じて、前記権利書データの正当性を証明する。

このとき、前記管理装置による前記権利書データの正当性の証明は、例えば、 権利書データに対しての前記管理装置の署名データを作成することによって行われる。

第11の発明のデータ提供システムでは、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ提供装置から前記データ 処理装置に配給する。

次に、前記データ処理装置において、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行う。

また、前記データ提供装置からの要求に応じて、前記管理装置において前記権利書データの正当性を証明する。

また、第11の発明のデータ提供システムは、好ましくは、前記データ提供装置は、前記権利書データと、自らの識別子と、少なくとも前記権利書データに対して自らの秘密鍵データを用いて作成した署名データとを格納したモジュールを前記管理装置に送信して前記要求を行う。

また、第11の発明のデータ提供システムは、好ましくは、前記管理装置は、前記データ提供装置の前記秘密鍵データに対応する公開鍵データの正当性を証明する公開鍵証明書データを、自らの秘密鍵データを用いて作成した署名データと共に、前記データ提供装置に配給し、前記データ提供装置は、前記公開鍵証明書データと、前記権利書データと、自らの識別子と、前記署名データとを格納したモジュールを前記管理装置に送信して前記要求を行う。

また、第11の発明のデータ提供システムは、好ましくは、前記管理装置は、配信鍵データを管理し、当該配信鍵データを前記データ処理装置に配給し、前記データ提供装置からの要求に応じて、前記権利書データに対して自らの秘密鍵データを用いて作成した署名データを生成し、当該生成した署名データと前記権利書データとを格納したモジュールを前記配信鍵データを用いて暗号化して前記データ提供装置に送信し、前記データ提供装置は、前記管理装置から受信したモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記データ提供装置から受信した前記モジュールを、前記配信鍵データを用いて復号し、当該モジュールに格納された前記署名データの正当性を前記管理装置の公開鍵データを用いて検証し、正当であると判断した場合に、前記モジュールに格納された権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行う。

また、第12の発明のデータ提供システムは、データ提供装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを前記データ処理装置に配給し、前記コンテンツ鍵データの正当性を証明することを前記管理装置に要求し、前記データ処理装置は、前記配給を受けたコンテンツデータを、前記コンテンツ鍵データを用いて復号し、当該復号したコンテンツデータを利用し、前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、前記データ提供装置からの要求に応じて、前記コンテンツ鍵データの正当性を証明する。

第12の発明のデータ提供システムでは、前記データ提供装置から前記データ 処理装置に、コンテンツ鍵データを用いて暗号化したコンテンツデータを配給す る。

次に、前記データ処理装置において、、前記配給を受けたコンテンツデータを 、前記コンテンツ鍵データを用いて復号し、当該復号したコンテンツデータを利 用する。

また、前記データ提供装置からの要求に応じて、前記管理装置において前記コンテンツ鍵データの正当性を証明する。

また、第13の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記権利書データの正当性を証明することを前記管理装置に要求し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行い、前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、前記データ提供装置からの要求に応じて、前記権利書データの正当性を証明する。

第13の発明のデータ提供システムでは、前記データ提供装置から前記データ 処理装置に、コンテンツ鍵データを用いて暗号化したコンテンツデータを配給す る。

次に、前記データ処理装置において、前記配給を受けたコンテンツデータを、 前記コンテンツ鍵データを用いて復号し、当該復号したコンテンツデータを利用 する。

また、前記データ提供装置からの要求に応じて、前記管理装置において前記コンテンツ鍵データの正当性を証明する。

第14の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記コンテンツ鍵データの正当性を証明することを前記管理装置に要求し、前記データ配給装置は、前記提供されたコン

テンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた権利書データに基づいて、前記コンテンツ鍵データを用いた前記コンテンツデータの復号を含む前記コンテンツデータの利用を行い、前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、前記データ提供装置からの要求に応じて、前記コンテンツ鍵データの正当性を証明する。

第14の発明のデータ提供システムでは、前記データ提供装置から前記データ 配給装置に、コンテンツ鍵データを用いて暗号化したコンテンツデータと、当該 コンテンツデータの取り扱いを示す権利書データとを提供する。

次に、前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給する。

次に、前記データ処理装置において、前記配給を受けた権利書データに基づいて、前記コンテンツ鍵データを用いた前記コンテンツデータの復号を含む前記コンテンツデータの利用を行う。

また、前記データ提供装置からの要求に応じて、前記管理装置において、前記コンテンツ鍵データの正当性を証明する。

また、第15の発明の管理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを配給するデータ提供装置と、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行うデータ処理装置とを管理する管理装置であって、前記データ提供装置からの要求に応じて、前記権利書データの正当性を証明する。

また、第16の発明の管理装置は、コンテンツ鍵データを用いて暗号化したコンテンツデータ、および当該コンテンツデータの取り扱いを示す権利書データを配給するデータ提供装置と、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータを前記コンテンツ鍵データを用いて復号した後に当該コンテンツデータの利用を行うデータ処理装置とを管理する管理装置であっ

て、前記データ提供装置からの要求に応じて、前記コンテンツ鍵データの正当性 を証明する。

また、第17の発明の管理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを提供するデータ提供装置と、前記提供を受けた前記コンテンツデータおよび前記権利書データを配給するデータ配給装置と、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行うデータ処理装置とを管理する管理装置であって、前記データ提供装置からの要求に応じて、前記権利書データの正当性を証明する。

また、第18の発明のデータ提供方法は、データ提供装置、データ処理装置および管理装置を用いたデータ提供方法であって、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ提供装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行い、前記データ提供装置からの要求に応じて、前記管理装置において前記権利書データの正当性を証明する。

また、第19の発明のデータ提供方法は、データ提供装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを用いて暗号化したコンテンツデータを配給し、前記データ処理装置において、前記配給を受けたコンテンツデータを、前記コンテンツ鍵データを用いて復号し、当該復号したコンテンツデータを利用し、前記データ提供装置からの要求に応じて、前記管理装置において前記コンテンツ鍵データの正当性を証明する。

また、第20のい発明のデータ提供方法は、データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ 提供装置から前記データ配給装置に、コンテンツデータと、当該コンテンツデー タの取り扱いを示す権利書データとを提供し、前記データ配給装置から前記デー

夕処理装置に、前記提供されたコンテンツデータおよび前記権利書データを配給 し、前記データ処理装置において、前記配給を受けた権利書データに基づいて前 記配給を受けた前記コンテンツデータの利用を行い、前記データ提供装置からの 要求に応じて、前記管理装置において、前記権利書データの正当性を証明する。

また、第21の発明のデータ提供方法は、データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化したコンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供し、前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた権利書データに基づいて、前記コンテンツ鍵データを用いた前記コンテンツデータの復号を含む前記コンテンツデータの利用を行い、前記データ提供装置からの要求に応じて、前記管理装置において、前記コンテンツ鍵データの正当性を証明する。

また、第22の発明のデータ提供システムは、データ提供装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う。

第22の発明のデータ提供システムでは、前記データ提供装置から前記データ 処理装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利 書データとを配給する。

次に、データ処理装置において、前記配給を受けた権利書データに基づいて前 記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一 方を決定する。

次に、前記データ処理装置から管理装置に、当該決定した購入形態および利用 形態の少なくとも一方の履歴を示す履歴データを送信する。

次に、前記管理装置において、前記データ提供装置および前記データ処理装置を管理し、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う。

また、第23の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置と通信を行う第1のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第2のモジュールとを有し、前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配

するための利益分配処理を行う。

第23の発明のデータ提供システムでは、データ提供装置からデータ配給装置 に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データ とを提供する。

次に、前記データ配給装置からデータ処理装置に、前記提供されたコンテンツ データおよび前記権利書データを配給する。

次に、前記データ処理装置において、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する。

次に、前記データ処理装置から前記管理装置に、前記決定した購入形態および 利用形態の履歴を示す履歴データを送信する。

次に、前記管理装置において、受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う。

また、第24の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置から受信したデータ配給装置用購入履歴データに基づいて、前記コンテンツデータの配給に関する課金処理を行い、前記データ処理装置は、前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信する第1のモジュールと、前記配給を受けた前記権利書データに基づいて、前

記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す管理装置用履歴データを前記管理装置に送信する第2のモジュールとを有し、前記管理装置は、前記管理装置用履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴った得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配する利益分配処理を行う。

また、第25の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理する。

また、第26の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理するデータ提供システムであって、前記データ提供装置、前記データ配給装置、前記データ処理装置および前記管理装置との間でのデータの伝送を、公開鍵暗号化方式を用いた相互認証、署名生成、署名検証と、共通鍵暗号化方式よるデータの暗号化とを用いて行う。

また、第27の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供された

コンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、前記管理装置は、前記データ提供装置、前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理するデータ提供システムであって、前記データ提供装置、前記データ配給装置および前記データ処理装置は、他の装置との間で通信を行う前に、前記管理装置から自らの前記公開鍵証明書データを取得し、当該取得した公開鍵証明書データを前記他の装置に送信する。

また、第28の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを供給するときに、当該データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対

応する公開鍵データの公開鍵証明書データを作成および管理するデータ提供システムであって、前記データ提供装置、前記データ配給装置および前記データ処理装置は、他の装置との間で通信を行う際に、前記管理装置から自らの前記公開鍵証明書データを取得し、当該取得した公開鍵証明書データを前記通信時に前記他の装置に送信する。

また、第29の発明のデータ提供システムは、データ提供装置、データ配給装 置、データ処理装置および管理装置を有し、前記データ提供装置は、コンテンツ データを前記データ配給装置に提供し、前記データ配給装置は、前記提供された コンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記 配給を受けた前記コンテンツデータを利用し、前記管理装置は、前記データ提供 装置、前記データ配給装置および前記データ処理装置によるデータ提供サービス の運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処 理装置の各々が、他の装置にデータを供給するときに、当該データが自らによっ て作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の 装置からデータの供給を受けたときに、当該データに対応する署名データの正当 性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置 、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対 応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公 開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書 破棄データを生成し、前記データ提供装置、前記データ配給装置および前記デー 夕処理装置が前記公開鍵証明書破棄データが特定する公開鍵証明書データを用い た前記通信または前記配給を行うことを規制する。

また、第30の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記管理装置は、前記データ

提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ提供装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ処理装置に配給し、前記データ処理装置は、前記管理装置から前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを提供した前記データ提供装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記配給を受けたコンテンツデータの利用を制御する。

また、第31の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ提供装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを特定する公開鍵証明書破棄データを特定する公開鍵証明書破棄データを特定する公開鍵証明書破棄データに基づいて、前記提供を受けたコンテンツデータを提供した前記データ提供装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記提供されたコンテンツデータの前記データ処理装置への配給

を制御する。

また、第32の発明のデータ提供システムは、データ提供装置、データ配給装 置、データ処理装置および管理装置を有し、前記管理装置は、前記データ提供装 置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの 運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当 該データが自らによって作成されたことを示す署名データを自らの秘密鍵データ を用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応 する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データ に対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成し た公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証 明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に 配給し、前記データ提供装置は、前記管理装置から前記配給を受けた公開鍵証明 書破棄データに基づいて、コンテンツデータの提供先のデータ配給装置の公開鍵 証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記デ ータ配給装置への前記コンテンツデータの提供を制御し、前記データ配給装置は 、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ 処理装置は、前記配給を受けたコンテンツデータを利用する。

また、第33の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証

明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータの提供し、前記データ配給装置は、前記提供されたコンテンツデータと、前記配給を受けた公開鍵証明書破棄データとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御する。

また、第34の発明のデータ提供システムは、データ提供装置、データ配給装 置、データ処理装置および管理装置を有し、前記管理装置は、前記データ提供装 置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの 運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当 該データが自らによって作成されたことを示す署名データを自らの秘密鍵データ を用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応 する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データ に対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成し た公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証 明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ処理装置に 配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータを提供 し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理 装置に配給し、前記データ処理装置は、前記配給を受けた公開鍵証明書破棄デー タに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装 置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づい て、前記配給を受けたコンテンツデータの利用を制御する。

また、第35の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記管理装置は、前記データ提供装

置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの 運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当 該データが自らによって作成されたことを示す署名データを自らの秘密鍵データ を用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応 する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データ に対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成し た公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証 明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に 配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータおよび 前記公開鍵証明書破棄データを直記データ処理装置に配給し、前記データを提供し、前記データ配給装置は、前記提供された コンテンツデータおよび公開鍵証明書破棄データを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証 明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御する。

また、第36の発明のデータ提供システムは、データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ処理装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータ

および前記公開鍵証明書破棄データを提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび公開鍵証明書破棄データを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置から配給を受けた公開鍵証明書破棄データに基づいて他のデータ処理装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記他のデータ処理装置との間の通信を制御する。

また、第37の発明のデータ提供システムは、データ提供装置、データ配給装 置、複数のデータ処理装置および管理装置を有し、前記管理装置は、前記データ 提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サー ビスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するとき に、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵 データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データ に対応する公開鍵データを用いて検証する場合に、前記データ処理装置の秘密鍵 データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記 作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公 開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給 装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータ を提供し、前記データ配給装置は、前記提供されたコンテンツデータと、前記配 給された公開鍵証明書破棄データとを前記データ処理装置に配給し、前記データ 処理装置は、前記データ配給装置から配給を受けた公開鍵証明書破棄データに基 づいて他のデータ処理装置の公開鍵証明書データが無効であるか否かを検証し、 当該検証の結果に基づいて前記他のデータ処理装置との間の通信を制御する。

また、第38の発明のデータ提供システムは、データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、前記データ処理装置は、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理 装置を示す登録データを前記管理装置に供給し、前記管理装置から供給された登

録データ内の破棄フラグを参照して、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを生成いて、前記データ処理装置から供給を受けた前記登録データ内の前記破棄フラグを設定して新たな登録データを生成し、当該生成した登録データを前記データ処理装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、前記データ配給装置は、前記データ配給装置にコンテンツデータを提供し、前記データ配給装置は、前記提供されたコンテンツデータの理装置に配給する。

また、第39の発明のデータ提供システムは、データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書でクを作成および管理し、前記作成した公開鍵証明書でクを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータおよび前記公開鍵証明書破棄データを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた公

開鍵証明書破棄データに基づいて、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データ内の破棄フラグを設定し、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制する。

また、第40の発明のデータ提供システムは、データ提供装置、データ配給装 置、複数のデータ処理装置および管理装置を有し、前記管理装置は、前記データ 提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サー ビスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するとき に、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成す る場合に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作 成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明 書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄デ ータを前記データ配給装置に配給し、前記データ提供装置は、前記データ配給装 置にコンテンツデータを提供し、前記データ配給装置は、前記提供されたコンテ ンツデータおよび前記公開鍵証明書破棄データを前記データ処理装置に配給し、 前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、 自らが接続された所定のネットワーク内に接続された既に登録された前記データ 処理装置を示す登録データ内の破棄フラグを設定し、当該破棄フラグによって無 効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の 通信を規制する。

また、第41の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置と通信を行う第1のモジュー

ルと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第2のモジュールとを有し、前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行い、当該利益分配処理の結果に基づいて決済を行う決済機能と、前記権利書データの登録を行う権利管理機能とを有する。

また、第42の発明のデータ提供システムは、データ提供装置、データ配給装 置、データ処理装置および管理装置を有するデータ提供システムであって、前記 データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示 す権利書データとを前記データ配給装置に提供し、前記データ配給装置は、前記 管理装置から配給を受けた決済請求権データを用いて決済処理を行う課金機能を 有し、前記提供されたコンテンツデータおよび前記権利書データを前記データ処 理装置に配給し、前記データ処理装置は、前記データ配給装置と通信を行う第1 のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受け た前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、 当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に 送信する第2のモジュールとを有し、前記管理装置は、データ提供装置、データ 配給装置およびデータ処理装置を管理し、前記第2のモジュールから受信した前 記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配 給を受けたこと、および、前記コンテンツデータを前記購入および前記利用した ことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関 係者に分配するための利益分配処理を行い、当該利益分配処理の結果に基づいて

決済行う際に用いられる決済請求権データを生成して前記データ配給装置に供給 する決済請求権データ生成機能と、前記権利書データの登録を行う権利管理機能 とを有する。

また、第43の発明のデータ提供システムは、データ提供装置、データ配給装 置、データ処理装置および管理装置を有するデータ提供システムであって、前記 データ提供装置は、前記管理装置から配給を受けた決済請求権データを用いて決 済処理を行う課金機能を有し、コンテンツデータと、当該コンテンツデータの取 り扱いを示す権利書データとを前記データ配給装置に提供し、前記データ配給装 **置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処** 理装置に配給し、前記データ処理装置は、前記データ配給装置と通信を行う第1 のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受け た前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、 当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に 送信する第2のモジュールとを有し、前記管理装置は、データ提供装置、データ 配給装置およびデータ処理装置を管理し、前記第2のモジュールから受信した前 記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配 給を受けたこと、および、前記コンテンツデータを前記購入および前記利用した ことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関 係者に分配するための利益分配処理を行い、当該利益分配処理の結果に基づいて 決済行う際に用いられる決済請求権データを生成して前記データ提供装置に配給 する決済請求権データ生成機能と、前記権利書データの登録を行う権利管理機能 とを有する。

また、第44の発明の管理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを配給するデータ提供装置と、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態

の少なくとも一方の履歴を示す履歴データを生成するデータ処理装置とを管理する管理装置であって、前記履歴データを前記データ処理装置から受信し、当該受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を前記データ提供装置の関係者に分配するための利益分配処理を行う。

また、第45の発明の管理装置は、コンチンツデータと当該コンテンツデータの取り扱いを示す権利書データとを提供するデータ提供装置と、前記提供を受けた前記コンテンツデータおよび前記権利書データを配給するデータ配給装置と、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを生成するデータ処理装置とを管理する管理装置であって、受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う。

また、第46の発明のデータ処理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとの配給をデータ提供装置から受け、当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益を前記データ提供装置の関係者に分配するための利益分配処理を所定の履歴データに基づいて行う管理装置に前記履歴データを送信するデータ処理装置であって、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す前記履歴データを前記管理装置に送信する。

また、第47の発明のデータ処理装置は、コンテンツデータと当該コンテンツ データの取り扱いを示す権利書データとの提供をデータ提供装置から受けたデー

夕配給装置から、前記コンテンツデータおよび前記権利書データの配給を受け、 当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益 を前記データ提供装置および前記データ配給装置の関係者に分配するための利益 分配処理を所定の履歴データに基づいて行う管理装置に前記履歴データを送信す るデータ処理装置であって、前記データ配給装置と通信を行う第1のモジュール と、前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コン テンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定し た購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第 2のモジュールとを有する。

また、第48の発明のデータ処理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとの配給をデータ配給装置を介してデータ提供装置から受け、当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を前記管理装置用履歴データに基づいて行う管理装置に前記履歴データを送信するデータ処理装置であって、前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信する第1のモジュールと、前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す前記管理装置用履歴データを前記管理装置に送信する第2のモジュールとを有する。

また、第49の発明のデータ提供方法は、データ提供装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ処理装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを配給し、前記データ処理装置において、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利

用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、前記管理装置において、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う。

また、第50の発明のデータ提供方法は、データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ配給装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供し、前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを配給し、前記データ処理装置において、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信し、前記管理装置において、前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う。

また、第51の発明のデータ提供方法は、データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ配給装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供し、前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置において、前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信し、前記配給を受けた前記権

利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す管理装置用履歴データを前記管理装置に送信し、前記管理装置において、前記管理装置用履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴った得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配し、前記データ配給装置において、前記データ処理装置から受信したデータ配給装置用購入履歴データに基づいて、前記コンテンツデータの配給に関する課金処理を行う。

#### 図面の簡単な説明

図1は、本発明の第1実施形態のEMDシステムの全体構成図である。

図2は、図1に示すコンテンツプロバイダの機能プロック図であり、ユーザホームネットワークのSAMとの間で送受信されるデータに関連するデータの流れを示す図である。

図3は、図1に示すコンテンツプロバイダの機能ブロック図であり、コンテンツプロバイダとEMDサービスセンタとの間で送受信されるデータに関連するデータの流れを示す図である。

図4は、図1に示すコンテンツプロバイダからSAMに送信されるセキュアコンテナのフォーマットを説明するための図である。

図5は、OSIレイヤ層と、本実施形態のセキュアコンテナの定義との対応関係を説明するための図である。

図6は、ROM型の記録媒体を説明するための図である。

図7AはコンテンツプロバイダからEMDサービスセンタに送信される権利登録要求用モジュールのフォーマットを説明するための図、図7BはEMDサービスセンタからコンテンツプロバイダに送信される権利化証明書モジュールを説明するための図である。

図8は、第1実施形態において、コンテンツプロバイダが、EMDサービスセンタに、自らの秘密鍵データに対応する公開鍵データの正当性を証明する公開鍵 証明書データを要求する場合の処理のフローチャートである。

図 9 は、第 1 実施形態において、コンテンツプロバイダがユーザホームネット ワークのSAMにセキュアコンテナを送信する場合の処理のフローチャートであ る。

図10は、図1に示すEMDサービスセンタの機能プロック図であり、コンテンツプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

図11は、図1に示すEMDサービスセンタの機能プロック図であり、SAMおよび図1に示す決済機関との間で送受信されるデータに関連するデータの流れを示す図である。

図12は、第1実施形態において、EMDサービスセンタがコンテンツプロバイダから公開鍵証明書データの発行要求を受けた場合の処理のフローチャートである。

図13は、第1実施形態において、EMDサービスセンタがSAMから、公開 鍵証明書データの発行要求を受けた場合の処理のフローチャートである。

図14は、第1実施形態において、EMDサービスセンタがコンテンツプロバイダから権利書データおよびコンテンツ鍵データの登録要求を受けた場合の処理のフローチャートである。

図15は、第1実施形態において、EMDサービスセンタが決済処理を行なう場合の処理のフローチャートである。

図16は、図1に示すユーザホームネットワーク内のネットワーク機器の構成 図である。

図17は、図1に示すユーザホームネットワーク内のSAMの機能プロック図であり、コンテンツプロバイダから受信したセキュアコンテナを復号するまでの

データの流れを示す図である。

図18は、図16に示す外部メモリに記憶されるデータを説明するための図である。

図19は、スタックメモリに記憶されるデータを説明するための図である。

図20は、図1に示すユーザホームネットワーク内のネットワーク機器のその 他の構成図である。

図21は、図17に示す記憶部に記憶されるデータを説明するための図である

図22は、第1実施形態において、セキュアコンテナをコンテンツプロバイダから入力し、セキュアコンテナ内のキーファイルKFを復号する際のSAM内での処理のフローチャートである。

図23は、図1に示すユーザホームネットワーク内のSAMの機能プロック図であり、コンテンツデータを利用・購入する処理などに関連するデータの流れを示す図である。

図24は、第1実施形態において、コンテンツプロバイダからダウンロードメモリにダウンロードされたセキュアコンテナの購入形態を決定するまでの処理のフローチャートである。

図25は、第1実施形態において、ダウンロードメモリに記憶されている購入 形態が既に決定されたコンテンツデータを再生する場合の処理のフローチャート である。

図26は、図16に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、AV機器のSAMに転送する場合の転送元のSAM内での処理の流れを説明するための図である。

図27は、図26に示す場合における転送元のSAM内でのデータの流れを示す図である。

図28は、第1実施形態において、ネットワーク機器のダウンロードメモリに

ダウンロードされた既に購入形態が決定されたコンテンツファイルおよびキーファイルを、他のAV機器のSAMに転送する場合のSAM内での処理のフローチャートである。

図29は、購入形態が決定したセキュアコンテナのフォーマットを説明するための図である。

図30は、図26に示す場合において、転送先のSAMにおいて、入力したコンテンツファイルなどを、RAM型あるいはROM型の記録媒体(メディア)に書き込む際のデータの流れを示す図である。

図31は、第1実施形態において、他のSAMから入力したコンテンツファイルなどを、RAM型などの記録媒体に書き込む際のSAM内での処理のフローチャートである。

図32、コンテンツの購入形態が未決定の図6に示すROM型の記録媒体をユーザホームネットワークがオフラインで配給を受けた場合に、AV機器において購入形態を決定する際の処理の流れを説明するための図である。

図33は、図32に示す場合において、SAM内でのデータの流れを示す図である。

図34は、第1実施形態において、コンテンツの購入形態が未決定の図5に示すROM型の記録媒体をユーザホームネットワークがオフラインで配給を受けた場合に、AV機器において購入形態を決定する際の処理のフローチャートである

. 図35は、図34のフローチャートの続きのフローチャートである。

図36は、ユーザホームネットワーク内のAV機器において購入形態が未決定のROM型の記録媒体からセキュアコンテナを読み出して、これを他のAV機器に転送してRAM型の記録媒体に書き込む際の処理の流れを説明するための図である。

図37は、図36に示すように、第1のAV機器において購入形態が未決定の

ROM型の記録媒体からセキュアコンテナを読み出して第2のAV機器に転送し、第2のAV機器において購入形態を決定してRAM型の記録媒体に書き込む際の第1のAV機器の処理のフローチャートである。

図38は、図37に示す場合の第2のAV機器の処理のフローチャートである

図39は、図38に示すフローチャートの続きのフローチャートである。

図40は、図36に示す場合における転送元のSAM内でのデータの流れを示す図である。

図41は、図36に示す場合における転送先のSAM内でのデータの流れを示す図である。

図42は、図1に示すコンテンツプロバイダ、EMDサービスセンタおよびSAMの相互間で、イン・バント方式およびアウト・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

図43は、図1に示すコンテンツプロバイダ、EMDサービスセンタおよびSAMの相互間で、イン・バント方式およびアウト・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

図44は、バスへの機器の接続形態の一例を説明するための図である。

図45は、SAM登録リストのデータフォーマットを説明するための図である

図46は、図1に示すコンテンツプロバイダの全体動作のフローチャートである。

図47は、本発明の第1実施形態の第2変形例を説明するための図である。

図48は、本発明の第1実施形態の第3変形例を説明するための図である。

図49は、本発明の第2実施形態のEMDシステムの全体構成図である。

図50は、図49に示すコンテンツプロバイダの機能プロック図であり、サービスプロバイダに送信されるセキュアコンテナに関するデータの流れを示す図で

ある。

図51は、図49に示すサービスプロバイダの機能プロック図であり、ユーザホームネットワークとの間で送受信されるデータの流れを示す図である。

図52は、第2実施形態において、コンテンツプロバイダから供給を受けたセキュアコンテナからセキュアコンテナを作成し、これをユーザホームネットワークに配給する際のサービスプロバイダの処理のフローチャートである。

図53は、図49に示すサービスプロバイダからユーザホームネットワークに 送信されるセキュアコンテナのフォーマットを説明するための図である。

図54は、図49に示すサービスプロバイダの機能プロック図であり、EMD サービスセンタとの間で送受信されるデータの流れを示す図である。

図55は、サービスプロバイダからEMDサービスセンタに送信されるプライスタグ登録要求用モジュールのフォーマットを説明するための図である。

図56は、図49に示すEMDサービスセンタの機能プロック図であり、サービスプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

図57は、図49に示すEMDサービスセンタの機能プロック図であり、コンテンツプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

図58は、図49に示すEMDサービスセンタの機能プロック図であり、SAMとの間で送受信されるデータに関連するデータの流れを示す図である。

. 図59は、利用履歴データの内容を説明するための図である。

図60は、第2実施形態において、EMDサービスセンタがサービスプロバイダから公開鍵証明書データの発行要求を受けた場合の処理のフローチャートである。

図61は、第2実施形態において、EMDサービスセンタが、サービスプロバイダからプライスタグデータの登録要求を受けた場合の処理のフローチャートで

ある。

図62は、第2実施形態において、EMDサービスセンタが決済を行なう場合の処理のフローチャートである。

図63は、図49に示すネットワーク機器の構成図である。

図64は、図63に示すCAモジュールの機能プロック図である。

図65は、図63に示すSAMの機能プロック図であり、セキュアコンテナを 入力してから復号するまでのデータの流れを示す図である。

図66は、図65に示す記憶部に記憶されるデータを説明するための図である

図67は、図63に示すSAMの機能プロック図であり、コンテンツの購入・ 利用形態を決定する場合などのデータの流れを示す図である。

図68は、第2実施形態において、セキュアコンテナをサービスプロバイダから入力し、セキュアコンテナ内のキーファイルを復号する際のSAMの処理のフローチャートである。

図69は、第2実施形態において、サービスプロバイダからダウンロードメモリにダウンロードされたセキュアコンテナの購入形態を決定するまでのSAMの処理のフローチャートである。

図70は、ダウンロードメモリに記憶されている購入形態が既に決定されたコンテンツデータを再生する場合の処理のフローチャートである。

図71は、購入形態が決定された後のキーファイルのフォーマットを説明する ための図である。

図72は、図63に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、AV機器のSAMに転送する場合の転送先のSAM内での処理の流れを説明するための図である。

図49は、図72に示す場合の転送元のSAM内でのデータの流れを示す図である。

図74は、図72に示すように、例えば、ネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、AV機器のSAMに転送する場合の転送元のSAMの処理のフローチャートである

図75は、ネットワーク機器のSAMからAV機器のSAMに転送される購入 形態が既に決定されたセキュアコンテナのフォーマットを説明するための図である。

図76は、図72に示す場合の転送先のSAM内でのデータの流れを示す図である。

図77は、図72に示すように、他のSAMから入力したコンテンツファイルなどを、RAM型などの記録媒体に書き込む際のSAMの処理のフローチャートである。

図78は、図49に示すEMDシステムの全体動作のフローチャートである。

図79は、図49に示すEMDシステムの全体動作のフローチャートである。

図80は、本発明の第2実施形態の第1変形例に係わる2個のサービスプロバイダを用いたEMDシステムの構成図である。

図81は、本発明の第2実施形態の第2変形例に係わる複数のコンテンツプロバイダを用いたEMDシステムの構成図である。

図82は、本発明の第2実施形態の第3変形例に係わるEMDシステムの構成 図である。

図83は、本発明の第2実施形態の第4変形例に係わるEMDシステムの構成 図である。

図84は、公開鍵証明書データの取得ルートの形態を説明するための図である

図85は、コンテンツプロバイダの公開鍵証明書データを無効にする場合の処理を説明するための図である。

図86は、サービスプロバイダの公開鍵証明書データを無効にする場合の処理 を説明するための図である。

図87は、SAMの公開鍵証明書データを無効にする場合の処理を説明するための図である。

図88は、SAMの公開鍵証明書データを無効にする場合のその他の処理を説明するための図である。

図89は、図49に示すEMDシステムにおいて、EMDサービスセンタの代わりに権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを設けた場合を説明するための図である。

図90は、図89に示す権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを単体のEMDサービスセンタ内に設けた場合のEMDシステムの構成図である。

図91は、サービスプロバイダが電子決済用クリアリングハウスに直接的に決済を行う場合のEMDシステムの構成図である。

図92は、コンテンツプロバイダが電子決済用クリアリングハウスに直接的に 決済を行う場合のEMDシステムの構成図である。

図93は、本発明の第2実施形態の第8変形例において、図49に示すコンテンツプロバイダからサービスプロバイダに提供されるセキュアコンテナのフォーマットを説明するための図である。

図94は、図93に格納されたモジュールの詳細なフォーマットを説明するための図である。

図 9 5 は、本発明の第 2 実施形態の第 8 変形例において、図 4 9 に示すサービスプロバイダから S A M に提供されるセキュアコンテナのフォーマットを説明するための図である。

図96は、インターネットを用いてセキュアコンテナを提供する場合の概念図である。

図 9 7 は、インターネットを用いてセキュアコンテナを提供する場合のその他の概念図である。

図98は、デジタル放送を用いてセキュアコンテナを提供する場合の概念図で ある。

図99は、デジタル放送を用いてセキュアコンテナを提供する場合のその他の 概念図である。

図100は、従来のEMDシステムの構成図である。

## 発明を実施するための最良の形態

以下、本発明の実施形態に係わるEMD(Electronic Music Distribution: 電子音楽配信)システムについて説明する。

本実施形態において、ユーザに配信されるコンテンツ(Content) データとは、音楽データ、映像データおよびプログラムなど情報そのものが価値を有するデジタルデータをいい、以下、音楽データを例に説明する。

## 第1実施形態

図1は、本実施形態のEMDシステム100の構成図である。

図1に示すように、EMDシステム100は、コンテンツプロバイダ101、EMDサービスセンタ(クリアリング・ハウス、以下、ESCとも記す)102 およびユーザホームネットワーク103を有する。

ここで、コンテンツプロバイダ101、EMDサービスセンタ102およびSAM1051~1054が、それぞれ本発明のデータ提供装置、管理装置およびデータ処理装置に対応している。

先ず、EMDシステム100の概要について説明する。

EMDシステム100では、コンテンツプロバイダ101は、自らが提供しよ

うとするコンテンツのコンテンツデータCの使用許諾条件などの権利内容を示す権利書(UCP:Usage Control Policy)データ106を、高い信頼性のある権威機関であるEMDサービスセンタ102に送信する。権利書データ106は、EMDサービスセンタ102によって権威化(認証)される。

また、コンテンツプロバイダ101は、コンテンツ鍵データKcでコンテンツデータCを暗号化してコンテンツファイルCFを生成すると共に、コンテンツ鍵データKcをEMDサービスセンタ102から配給された対応する期間の配信用鍵データKD1~KD5。で暗号化する。そして、コンテンツプロバイダ101は、暗号化されたコンテンツ鍵データKcおよびコンテンツファイルCFと自らの署名データとを格納(カプセル化)したセキュアコンテナ(本発明のモジュール)104を、インターネットなどのネットワーク、デジタル放送あるいは記録媒体などを用いて、ユーザホームネットワーク103に配給する。

このように、本実施形態では、デジタルのコンテンツデータCをカプセル化して提供することで、従来の記録媒体と密着したデジタルコンテンツを、記録媒体から切り離して、デジタルコンテンツ単体に存在価値を持たせることができる。

ここで、セキュアコンテナは、どのような流通経路(配送チャンネル)を介して提供されても、コンテンツデータC(商品)を販売するときの最も基本となる商品カプセルである。具体的には、セキュアンテナは、課金を行うための暗号情報や、コンテンツデータCの中身の正当性、コンテンツデータを作成した者の正当性およびコンテンツデータの流通業者の正当性を検証するための署名データや、コンテンツデータに埋め込む電子透かし情報に関する情報などの著作権に係わる情報を含む商品カプセルである。

ユーザホームネットワーク 103 は、例えば、ネットワーク機器 160 におよび AV 機器 160 ~ 160 を有する。

ネットワーク機器 1 6 0 1 は、SAM(Secure Application Module) 1 0 5 1 を内蔵している。

AV機器 $160_2 \sim 160_4$  は、それぞれSAM $105_2 \sim 105_4$  を内蔵している。SAM $105_1 \sim 105_4$  相互間は、例えば、IEEE(Institute of Electrical and Electronics Engineers) 1394シリアルインタフェースバスなどのバス191を介して接続されている。

SAM1051~105.は、ネットワーク機器1601がコンテンツプロバイダ101からネットワークなどを介してオンラインで受信したセキュアコンテナ104、および/または、コンテンツプロバイダ101からAV機器1602~160.に記録媒体を介してオフラインで供給されたセキュアコンテナ104を対応する期間の配信用鍵データKD1~KDsを用いて復号した後に、署名データの検証を行う。

SAM105 $_1$ ~10

SAM1051~1054は、上述したセキュアコンテナ104の購入・利用の履歴を利用履歴(Usage Log) データ108として記録する。

利用履歴データ108は、例えば、EMDサービスセンタ102からの要求に 応じて、ユーザホームネットワーク103からEMDサービスセンタ102に送 信される。

EMDサービスセンタ102は、利用履歴データ108に基づいて、課金内容を決定(計算)し、その結果に基づいて、ペイメントゲートウェイ90を介して銀行などの決済機関91に決済を行なう。これにより、ユーザホームネットワーク103のユーザが決済機関91に支払った金銭が、EMDサービスセンタ102による決済処理によって、コンテンツプロバイダ101に支払われる。

また、EMDサービスセンタ102は、一定期間毎に、決済レポートデータ107をコンテンツプロバイダ101に送信する。

本実施形態では、EMDサービスセンタ102は、認証機能、鍵データ管理機能および権利処理(利益分配)機能を有している。

すなわち、EMDサービスセンタ102は、中立の立場にある最高の権威機関であるルート認証局92に対しての(ルート認証局92の下層に位置する)セカンド認証局(Second Certificate Authority)としての役割を果たし、コンテンツプロバイダ101およびSAM1051~1051において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、EMDサービスセンタ102の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、EMDサービスセンタ102は、コンテンツプロバイダ101の権利書データ106を登録して権威化することも、EMDサービスセンタ102の認証機能の一つである。

また、EMDサービスセンタ 102は、例えば、配信用鍵データ $KD_1 \sim KD$ 。などの鍵データの管理を行なう鍵データ管理機能を有する。

また、EMDサービスセンタ102は、権威化した権利書データ106に記述された標準小売価格SRP(Suggested Retailer' Price) とSAM105 $_1$  ~SAM105 $_2$  から入力した利用履歴データ108とに基づいて、ユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ101に分配する権利処理(利益分配)機能を有する。

以下、コンテンツプロバイダ101の各構成要素について詳細に説明する。

[コンテンツプロバイダ101]

また、図3には、コンテンツプロバイダ101とEMDサービスセンタ102 との間で送受信されるデータに関連するデータの流れが示されている。

なお、図3以降の図面では、署名データ処理部、および、セッション鍵データ

KsBs を用いた暗号化・復号部に入出力するデータの流れは省略している。

図2および図3に示すように、コンテンツプロバイダ101は、コンテンツマスタソースサーバ111、電子透かし情報付加部112、圧縮部113、暗号化部114、乱数発生部115、暗号化部116、署名処理部117、セキュアコンテナ作成部118、セキュアコンテナデータベース118a、記憶部119、相互認証部120、暗号化・復号部121、権利書データ作成部122、SAM管理部124およびEMDサービスセンタ管理部125を有する。

コンテンツプロバイダ101は、EMDサービスセンタ102との間で通信を行う前に、例えば、自らが生成した公開鍵データ、自らの身分証明書および銀行口座番号 (決済を行う口座番号)をオフラインでEMDサービスセンタ102に登録し、自らの識別子 (識別番号) CP\_IDを得る。また、コンテンツプロバイダ101は、EMDサービスセンタ102から、EMDサービスセンタ102の公開鍵データと、ルート認証局92の公開鍵データとを受ける。

以下、図2および図3に示すコンテンツプロバイダ101の各機能プロックについて説明する。

コンテンツマスタソースサーバ111は、ユーザホームネットワーク103に 提供するコンテンツのマスタソースであるコンテンツデータを記憶し、提供しよ うとするコンテンツデータS111を電子透かし情報付加部112に出力する。

電子透かし情報付加部112は、コンテンツデータS111に対して、ソース電子透かし情報(Source Watermark)Ws、コピー管理用電子透かし情報(Copy Control Watermark)Wcおよびユーザ電子透かし情報(User Watermark)Wuなどを埋め込んでコンテンツデータS112を生成し、コンテンツデータS112を圧縮部113に出力する。

ソース電子透かし情報Wsは、コンテンツデータの著作権者名、ISRCコード、オーサリング日付、オーサリング機器ID(Identification Data)、コンテンツの配給先などの著作権に関する情報である。コピー管理用電子透かし情報W

cは、アナログインタフェース経由でのコピー防止用のためのコピー禁止ビットを含む情報である。ユーザ電子透かし情報Wuには、例えば、セキュアコンテナ 104の配給元および配給先を特定するためのコンテンツプロバイダ 101の識別子 $CP_ID$ およびユーザホームネットワーク 103の $SAM1051\sim10$  54の識別子 $SAM_ID1\sim SAM_ID4$  が含まれる。

また、電子透かし情報付加部112は、必要であれば、検索エンジンでコンテンツデータの検索を行うためのリンク用のIDを電子透かし情報としてコンテンツデータS111に埋め込む。

本実施形態では、好ましくは、各々の電子透かし情報の情報内容と埋め込み位置とを、電子透かし情報管理データとして定義し、EMDサービスセンタ102において電子透かし情報管理データを管理する。電子透かし情報管理データは、例えば、ユーザホームネットワーク103内のネットワーク機器1601およびAV機器1602~1604が、電子透かし情報の正当性を検証する際に用いられる。

例えば、ユーザホームネットワーク103では、電子透かし情報管理データに基づいて、電子透かし情報の埋め込み位置および埋め込まれた電子透かし情報の内容の双方が一致した場合に電子透かし情報が正当であると判断することで、偽りの電子透かし情報の埋め込みを高い確率で検出できる。

圧縮部113は、コンテンツデータS112を、例えば、ATRAC3(Adapt ive Transform Acoustic Coding 3) (商標) などの音声圧縮方式で圧縮し、圧縮したコンテンツデータS113を暗号化部114に出力する。

暗号化部114は、コンテンツ鍵データKcを共通鍵として用い、DES(Dat a Encryption Standard)やTriple DESなどの共通鍵暗号化方式で、コンテンツデータS113を暗号化してコンテンツデータCを生成し、これをセキュアコンテナ作成部118に出力する。

また、暗号化部114は、コンテンツ鍵データKcを共通鍵として用い、A/

V伸長用ソフトウェアSoftおよびメタデータMetaを暗号化した後に、セキュアコンテナ作成部117に出力する。

DESは、56ビットの共通鍵を用い、平文の64ビットを1ブロックとして 処理する暗号化方式である。DESの処理は、平文を攪拌し、暗号文に変換する 部分 (データ攪拌部)と、データ攪拌部で使用する鍵 (拡大鍵)データを共通鍵 データから生成する部分 (鍵処理部)とからなる。DESの全てのアルゴリズム は公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

先ず、平文の64ビットは、上位32ビットのH。と下位32ビットのL。とに分割される。鍵処理部から供給された48ビットの拡大鍵データK1および下位32ビットのL。を入力とし、下位32ビットのL。を撹拌したF関数の出力が算出される。F関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の2種類の基本変換から構成されている。次に、上位32ビットのH。と、F関数の出力との排他的論理和が算出され、その結果はL1とされる。また、L。は、H1とされる。

そして、上位32ビットのH。および下位32ビットのL。を基に、以上の処理を16回繰り返し、得られた上位32ビットのHisおよび下位32ビットのLisが暗号文として出力される。復号は、暗号化に使用した共通鍵データを用いて、上記の手順を逆さにたどることで実現される。

乱数発生部115は、所定ビット数の乱数を発生し、当該乱数をコンテンツ鍵データKcとして暗号化部114および暗号化部116に出力する。

なお、コンテンツ鍵データKcは、コンテンツデータが提供する楽曲に関する情報から生成してもよい。コンテンツ鍵データKcは、例えば、所定時間毎に更新される。

暗号化部116は、後述するようにしてEMDサービスセンタ102から受信されて記憶部119に記憶された配信用鍵データKD1~KD8のうち対応する

期間の配信用鍵データ $KD_1 \sim KD_8$ を入力し、当該配信用鍵データを共通鍵として用いたDESなどの共通暗号化方式によって図4Bに示すコンテンツ鍵データKc、権利書データ106、SAMプログラム・ダウンロード・コンテナSD $C_1 \sim SDC_8$  および署名・証明書モジュール $Mod_1$  を暗号化した後に、セキュアコンテナ作成部117に出力する。

署名・証明書モジュール $Mod_1$ には、図4Bに示すように、署名データ $SIG_2$ 、CP~ $SIG_4$ 、CP、コンテンツプロバイダ101の公開鍵データ $K_{CP,P}$ の公開鍵証明書 $CER_{CP}$ および当該公開鍵証明書 $CER_{CP}$ に対してのEMDサービスセンタ102の署名データ $SIG_1$ 、BSC が格納されている。

また、SAMプログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_8$  は、 $SAM105_1 \sim 105_4$  内でプログラムのダウンロードを行なう際に用いられる ダウンロード・ドライバと、権利書データ(UCP)U106のシンタックス(文法)を示すUCP-L(Label) . R(Reader)と、 $SAM105_1 \sim 105_4$  に 内蔵された記憶部(フラッシューROM)の書き換えおよび消去をプロック単位 でロック状態/非ロック状態にするためのロック鍵データとを格納している。

なお、記憶部119は、例えば、公開鍵証明書データを記憶するデータベース、配信用鍵データ $KD_1 \sim KD_8$ を記憶するデータベースおよびキーファイルKFを記憶するデータベースなどの種々のデータベースを備えている。

署名処理部 1 1 7 は、署名を行なう対象となるデータのハッシュ値をとり、コンテンツプロバイダ 1 0 1 の秘密鍵データ K cp. sを用いて、その署名データ S I Gを作成する。

なお、ハッシュ値は、ハッシュ関数を用いて生成される。ハッシュ関数は、対象となるデータを入力とし、当該入力したデータを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値(出力)から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシ

ュ値を持つ入力データを探し出すことが困難であるという特徴を有している。

セキュアコンテナ作成部118は、図4Aに示すように、ヘッダデータと、暗号化部114から入力したそれぞれコンテンツ鍵データKcで暗号化されたコンテンツデータC、A/V伸長用ソフトウェアSoftおよびメタデータMetaとを格納したコンテンツファイルCFを生成する。

ここで、A/V伸長用ソフトウェアSoftは、ユーザホームネットワーク103のネットワーク機器1601 およびAV機器1602 ~1604 において、コンテンツファイルCFを伸長する際に用いられるソフトウェアであり、例えば、ATRAC3方式の伸長用ソフトウェアである。

そして、セキュアコンテナ作成部118は、図4A, Bに示すコンテンツファイルCFおよびキーファイルKFと、図4Cに示すコンテンツプロバイダ101の公開鍵データKcpおよび署名データSIG1, BSc とを格納したセキュアコンテナ104を生成し、これをセキュアコンテナデータバース118aに格納した後に、ユーザからの要求に応じてSAM管理部124に出力する。

このように、本実施形態では、コンテンツプロバイダ101の公開鍵データKcp.pの公開鍵証明書CERcpをセキュアコンテナ104に格納してユーザホームネットワーク103に送信するイン・バンド(In-band) 方式を採用している。従って、ユーザホームネットワーク103は、公開鍵証明書CERcpを得るための通信をEMDサービスセンタ102との間で行う必要がない。

なお、本発明では、公開鍵証明書CERcpをセキュアコンテナ104に格納しないで、ユーザホームネットワーク103がEMDサービスセンタ102から公

開鍵証明書CERcrを得るアウト・オブ・バンド(Out-Of-band) 方式を採用してもよい。

相互認証部120は、コンテンツプロバイダ101がEMDサービスセンタ102およびユーザホームネットワーク103との間でオンラインでデータを送受信する際に、それぞれEMDサービスセンタ102およびユーザホームネットワーク103との間で相互認証を行ってセッション鍵データ(共有鍵)Ksbs を生成する。セッション鍵データKsbs は、相互認証を行う度に新たに生成される。

暗号化・復号部121は、コンテンツプロバイダ101がEMDサービスセンタ102およびユーザホームネットワーク103にオンラインで送信するデータを、セッション鍵データKsssを用いて暗号化する。

また、暗号化・復号部121は、コンテンツプロバイダ101がEMDサービスセンタ102およびユーザホームネットワーク103からオンラインで受信したデータを、セッション鍵データKsssを用いて復号する。

権利書データ作成部122は、権利書データ106を作成し、これを暗号化部116に出力する。

権利書データ106は、コンテンツデータCの運用ルールを定義した記述子(ディスクリプター)であり、例えば、コンテンツプロバイダ101の運用者が希望する標準小売価格SRP(Suggested Retailer' Price) やコンテンツデータCの複製ルールなどが記述されている。

SAM管理部124は、セキュアコンテナ104を、オフラインおよび/またはオンラインでユーザホームネットワーク103に供給する。

SAM管理部124は、CD-ROMやDVD(Digital Versatile Disc)などのROM型の記録媒体(メディア)を用いてセキュアコンテナ104をオフラインでユーザホームネットワーク103に配給する場合には、配信用鍵データKD1~KDeなどを用いてセキュアコンテナ104を暗号化して記録媒体に記録する。そして、この記録媒体は、販売などにより、ユーザホームネットワーク10

3にオフラインで供給される。

本実施形態では、セキュアコンテナ (商品カプセル) 104は、図5に示すように、OSIレイヤ層におけるアプリケーション層で定義される。また、プレゼンテーション層やトランスポート層に相当するカプセルは、セキュアコンテナを配送するための配送プロトコルとして、セキュアコンテナ104とは別に定義される。従って、セキュアコンテナ104を配送プロトコルに依存しないで定義できる。すなわち、セキュアコンテナ104を、例えばオンラインおよびオフラインの何れの形態でユーザホームネットワーク103に供給する場合でも、共通のルールに従って定義および生成できる。

例えば、セキュアコンテナ104をネットワークを使って供給する場合には、 セキュアコンテナ104をコンテンツプロバイダ101の領域で定義し、プレゼ ンテーション層およびトランスポート層をセキュアコンテナ104をユーザホー ムネットワーク103まで搬送するための搬送ツールと考える。

また、オフラインの場合に、ROM型の記録媒体を、セキュアコンテナ104 をユーザホームネットワーク103に搬送する搬送キャリアとして考える。

図6は、ROM型の記録媒体130を説明するための図である。

図 6 に示すように、R O M型の記録媒体 1 3 0 は、R O M領域 1 3 1、R A M 領域 1 3 2 およびメディア S A M 1 3 3 を有する。

ROM領域131には、図4Aに示したコンテンツファイルCFが記憶されている。

また、RAM領域132には、図4B、図4Cに示したキーファイルKFおよび公開鍵証明書データCER $c_P$ と機器の種類に応じて固有の値を持つ記録用鍵データ $K_{STR}$  とを引数としてMAC(Message Authentication Code) 関数を用いて生成したと署名データと、当該キーファイルKFおよび公開鍵証明書データCE $R_{CP}$ とを記録媒体に固有の値を持つメディア鍵データ $K_{MBD}$  を用いて暗号化したデータとが記憶される。

また、RAM領域132には、例えば、不正行為などで無効となったコンテンツプロバイダ101およびSAM105 $_1$  ~105 $_5$  を特定する公開鍵証明書破棄データ(リボケーションリスト)が記憶される。

また、また、RAM領域132には、後述するようにユーザホームネットワーク103のSAM105 $_1$ ~105 $_4$ においてコンテンツデータCの購入・利用形態が決定されたときに生成される利用制御状態(UCS)データ166などが記憶される。これにより、利用制御状態データ166がRAM領域132に記憶されることで、購入・利用形態が決定したROM型の記録媒体130となる。

メディアSAM133には、例えば、ROM型の記録媒体130の識別子であるメディアIDと、メディア鍵データKmgoとが記憶されている。

メディアSAM133は、例えば、相互認証機能を有している。

また、SAM管理部124は、セキュアコンテナ104を、ネットワークやデジタル放送などを用いてオンラインでユーザホームネットワーク103に配信する場合には、暗号化・復号部121においてセッション鍵データKsms を用いてセキュアコンテナ104を暗号化した後に、ネットワークを介してユーザホームネットワーク103に配信する。

本実施形態では、SAM管理部、EMDサービスセンタ管理部、並びに後述するコンテンツプロバイダ管理部およびサービスプロバイダ管理部として、例えば、内部の処理内容の監視(モニタリング)および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

ここで、コンテンツプロバイダ101からユーザホームネットワーク103へのコンテンツデータCの配給は、上述したように記録媒体130を用いて行う場合とネットワークを使ってオンラインで行う場合との何れでも権利書データ106が格納された共通の形式のセキュアコンテナ104を用いる。従って、ユーザホームネットワーク103のSAM1051~105.では、オフラインおよびオンラインの何れの場合でも、共通の権利書データ106に基づいた権利処理を

行なうことができる。

また、上述したように、本実施形態では、セキュアコンテナ104内に、コンテンツ鍵データKcで暗号化されたコンテンツデータCと、当該暗号化を解くためのコンテンツ鍵データKcとを同封するイン・バンド(In-Band)方式を採用している。イン・バンド方式では、ユーザホームネットワーク103の機器で、コンテンツデータCを再生しようとするときに、コンテンツ鍵データKcを別途配信する必要がなく、ネットワーク通信の負荷を軽減できるという利点がある。また、コンテンツ鍵データKcは配信用鍵データKD1  $\sim$ KD6 で暗号化されているが、配信用鍵データKD1  $\sim$ KD6 は、EMDサービスセンタ102で管理されており、ユーザホームネットワーク103のSAM1051  $\sim$ 1055 に事前に(SAM1051  $\sim$ 1056 がEMDサービスセンタ102に初回にアクセスする際に)配信されているので、ユーザホームネットワーク103では、EMDサービスセンタ102との間をオンラインで接続することなく、オフラインで、コンテンツデータCの利用が可能になる。

なお、本発明は、コンテンツデータCとコンテンツ鍵データKcとを別々に、 ユーザホームネットワーク103に供給するアウト・オブ・バンド(Out-Of-Band) 方式を採用できる柔軟性を有している。

EMDサービスセンタ管理部125は、EMDサービスセンタ102から6カ月分の配信用鍵データ $KD_1 \sim KD_6$  およびそれぞれに対応した署名データSI  $G_{KD_1, BSC} \sim SIG_{KD_6, BSC}$  と、コンテンツプロバイダ101の公開鍵データ $K_{CP, P}$ を含む公開鍵証明書 $CER_{CP}$ およびその署名データ $SIG_{1, BSC}$  と、決済レポートデータ107とを受信すると、これらを暗号化・復号部121においてセッション鍵データ $K_{SBS}$  を用いて復号した後に、記憶部119に記憶する。

決済レポートデータ107は、例えば、EMDサービスセンタ102が図1に 示す決済機関91に対して行なったコンテンツプロバイダ101に関する決済の 内容が記述されている。

また、EMDサービスセンタ管理部125は、提供するコンテンツデータCのグローバルユニーク(Global Unique) な識別子Content\_ID、公開鍵データKcp.pおよびそれらの署名データSIGs.cpを、EMDサービスセンタ102に送信し、EMDサービスセンタ102から、公開鍵データKcp.pの公開鍵証明書データCERcpを入力する。

また、EMDサービスセンタ管理部125は、権利書データ106をEMDサービスセンタ102に登録する際に、図7Aに示すように、提供するコンテンツデータCのグルーバルユニークな識別子Content\_ID、コンテンツ鍵データKcおよび権利書データ106を格納したモジュールModsと、その署名データSIGsсァとを格納した権利書登録要求用モジュールModsを作成し、これを暗号化・復号部121においてセッション鍵データKsвsを用いて暗号化した後に、ネットワークを介してEMDサービスセンタ102に送信する。 EMDサービスセンタ管理部125としては、前述したように、例えば、内部の処理内容の監視(モニタリング)および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

以下、図2および図3を参照しながら、コンテンツプロバイダ101における 処理の流れを説明する。

なお、以下に示す処理を行う前提として、コンテンツプロバイダ101の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、EMDサービスセンタ102に登録処理を行い、グローバルユニークな識別子CP\_IDを得ている。識別子CP\_IDは、記憶部119に記憶される。

以下、コンテンツプロバイダ101が、EMDサービスセンタ102に、自らの秘密鍵データ $K_{CP.}$ sに対応する公開鍵データ $K_{CP.}$ sの正当性を証明する公開鍵証明書データ $CER_{CP}$ を要求する場合の処理を図3および図8を参照しながら説明する。

図8は、当該処理のフローチャートである。

ステップSA1:コンテンツプロバイダ101は、例えば真性乱数発生器から 構成される乱数発生部115を用いて乱数を発生して秘密鍵データKcp.sを生成 する。

ステップSA2:コンテンツプロバイダ101は、秘密鍵データKcp, sに対応 する公開鍵データKcp, pを作成して記憶部119に記憶する。

ステップSA3:コンテンツプロバイダ101のEMDサービスセンタ管理部 125は、コンテンツプロバイダ101の識別子CP\_IDおよび公開鍵データ Kcp. pを記憶部119から読み出す。

そして、EMDサービスセンタ管理部125は、識別子CP\_IDおよび公開 鍵データKcp.pを含む公開鍵証明書データ発行要求をEMDサービスセンタ10 2に送信する。

ステップSA4:EMDサービスセンタ管理部125は、当該発行要求に応じて、公開鍵証明書データCERcpおよびその署名データSIG1、Bsc をEMDサービスセンタ102から入力して記憶部119に書き込む。

以下、コンテンツプロバイダ101が、EMDサービスセンタ102から配信用鍵データを受信する処理を図3を参照しながら説明する。

なお、以下に示す処理を行う前提として、コンテンツプロバイダ101は、EMDサービスセンタ102から既に公開鍵証明書データCERcpを得ている必要がある。

EMDサービスセンタ管理部 125が、EMDサービスセンタ 102から 6カ月分の配信用鍵データ  $KD_1 \sim KD_3$  およびその署名データ  $SIG_{KD1, BSC} \sim SIG_{KD1, BSC}$  を入力し、これを記憶部 119 内の所定のデータベースに記憶する

そして、署名処理部 1 1 7 において、記憶部 1 1 9 に記憶された署名データ S I  $G_{\text{KD1, BSC}} \sim S$  I  $G_{\text{KD6, BSC}}$  の正当性が確認された後に、記憶部 1 1 9 に記憶

されている配信用鍵データKD1~KDeが有効なものとして扱われる。

以下、コンテンツプロバイダ101がユーザホームネットワーク103のSA M1051にセキュアコンテナ104を送信する場合の処理を図2および図9を 参照しながら説明する。

図9は、当該処理のフローチャートである。

なお、以下の例では、コンテンツプロバイダ101からSAM1051にセキュアコンテナ104を送信する場合を例示するが、セキュアコンテナ104をSAM1052~1054に送信する場合も、SAM1051を介してSAM1052~1054に送信される点を除いて同じである。

ステップSB1:コンテンツデータS111がコンテンツマスタソースサーバ 111から読み出されて電子透かし情報付加部112に出力される。

電子透かし情報付加部112は、コンテンツデータS111に電子透かし情報を埋め込んでコンテンツデータS112を生成し、これを圧縮部113に出力する。

ステップSB2:圧縮部113は、コンテンツデータS112を、例えばAT RAC3方式で圧縮してコンテンツデータS113を作成し、これを暗号化部1 14に出力する。

ステップSB3: 乱数発生部115は、乱数を発生してコンテンツ鍵データKcを生成し、これを暗号化部114に出力する。

ステップSB4:暗号化部114は、コンテンツデータS113と、記憶部119から読み出されたメタデータMetaおよびA/V伸長用ソフトウェアSoftとを、コンテンツ鍵データKcを用いて暗号化してセキュアコンテナ作成部118に出力する。この場合に、メタデータMetaは暗号化しなくてもよい。

そして、セキュアコンテナ作成部118は、図4Aに示すコンテンツファイル CFを作成する。また、署名処理部117において、コンテンツファイルCFの

ハッシュ値がとられ、秘密鍵データKcp.sを用いて署名データSIGs.cpが生成される。

そして、セキュアコンテナ作成部118は、図4Bに示すキーファイルKFを作成する。

また、署名処理部117は、キーファイルKFのハッシュ値をとり、秘密鍵データKcp.sを用いて、署名データSIG7.cpを作成する。

ステップSB6:セキュアコンテナ作成部118は、図4Aに示すコンテンツファイルCFおよびその署名データSIG $_{6}$ ,  $c_{P}$ と、図4Bに示すキーファイルKFおよびその署名データSIG $_{7}$ ,  $c_{P}$ と、図4Cに示す公開鍵証明書データCER $_{CP}$ およびその署名データSIG $_{1,BSC}$ とを格納したセキュアコンテナ104を作成し、これを、セキュアコンテナデータベース118aに記憶する。

ステップSB7:セキュアコンテナ作成部118は、例えばユーザからの要求 (リクエスト) に応じてユーザホームネットワーク103に提供しようとするセキュアコンテナ104をセキュアコンテナデータベース118mから読み出して、相互認証部120とSAM1051 との間の相互認証によって得られたセッション鍵データKsbs を用いて暗号化・復号部121において暗号化した後に、SAM管理部124を介してユーザホームネットワーク103のSAM1051 に 送信する。

以下、コンテンツプロバイダ101が、EMDサービスセンタ102に権利書 データ106およびコンテンツ鍵データKcを登録して権威化することを要求する場合の処理を図3を参照して説明する。

権利書データ106およびコンテンツ鍵データKcの権威化要求処理は、個々のコンテンツデータC毎に行われる。

そして、図7Aに示す権利登録要求用モジュール $Mod_2$ を、相互認証部 120 と EMD サービスセンタ 102 との間の相互認証によって得られたセッション 鍵データ  $K_{SBS}$  を用いて暗号化・復号部 121 において暗号化した後に、EMD サービスセンタ管理部 125 から EMD サービスセンタ 102 に送信する。

本実施形態では、EMDサービスセンタ102において権利書データ106およびコンテンツ鍵データKcを権威化した後に、コンテンツプロバイダ101が EMDサービスセンタ102から権威化されたことを証明する権威化証明書モジュールを受信しない場合、すなわちコンテンツプロバイダ101において配信用鍵データKD<sub>1</sub>  $\sim$  KD<sub>8</sub> を用いて暗号化を行ってキーファイルKFを作成する場合を例示する。

但し、本発明は、例えば、EMDサービスセンタ102において権利書データ106およびコンテンツ鍵データKcを権威化した後に、EMDサービスセンタ102からコンテンツプロバイダ101に、配信用鍵データKD1~KD®を用いて暗号化した図7Bに示す権威化証明書モジュールMod2∞を送信してもよい

権威化証明書モジュールMod2aは、コンテンツデータCのグローバルユニー

クな識別子C o n t e n t  $\_$  I D、コンテンツ鍵データK c および権利書データ作成部 1 2 2 から入力した権利書データ 1 0 6 を格納したモジュールM o d s a と 、秘密鍵データK BSC、S を用いたモジュールM o d s a の署名データS I G s a BSC とを格納している。

この場合には、コンテンツプロバイダ 101は、例えば、セキュアコンテナ 104 内に、権威化証明書モジュール1000 100

なお、EMDサービスセンタ102は、それぞれ異なる月に対応する配信用鍵データ $KD_1 \sim KD_8$  を用いて暗号化した6カ月分の権威化証明書モジュールM od $_{2a}$ を生成し、これらをまとめてコンテンツプロバイダ101に送信してもよい。

[EMDサービスセンタ102]

EMDサービスセンタ102は、認証(CA:Certificate Authority)機能、 鍵管理(Key Management)機能および権利処理(Rights Clearing) (利益分配)機 能を有する。

図10は、EMDサービスセンタ102の機能の構成図である。

図10に示すように、EMDサービスセンタ102は、鍵サーバ141、鍵データベース141a、決算処理部142、署名処理部143、決算機関管理部144、証明書・権利書管理部145、CERデータベース145a、コンテンツプロバイダ管理部148、CPデータベース148a、SAM管理部149、SAMデータベース149a、相互認証部150および暗号化・復号部151を有する。

なお、図10には、EMDサービスセンタ102内の機能プロック相互間のデータの流れのうち、コンテンツプロバイダ101との間で送受信されるデータに 関連するデータの流れが示されている。

また、図11には、EMDサービスセンタ102内の機能プロック相互間のデ

-夕の流れのうち、SAM1051~1054 および図1に示す決済機関91との間で送受信されるデータに関連するデータの流れが示されている。

鍵サーバ141は、鍵データベース141aに記憶された各々有効期間が1カ 月の配信用鍵データを要求に応じて読み出してコンテンツプロバイダ管理部14 8およびSAM管理部149に出力する。

また、鍵データベース 141a 配信用鍵データ K D の他に、記録用鍵データ K STR 、メディア鍵データ K MAC などの鍵データを記憶する一連の鍵データースからなる。

決算処理部142は、SAM1051~105.から入力した利用履歴データ108と、証明書・権利書管理部145から入力した標準小売価格データSRPおよび販売価格とに基づいて決済処理を行い、決済レポートデータ107および決済請求権データ152を作成し、決済レポートデータ107をコンテンツプロバイダ管理部148に出力し、決済請求権データ152を決算機関管理部144に出力する。

なお、決算処理部 1 4 2 は、販売価格に基づいて、違法なダンピング価格による取り引きが行われたか否かを監視する。

ここで、利用履歴データ108は、ユーザホームネットワーク103における セキュアコンテナ104の購入、利用(再生、記録および転送など)の履歴を示 し、決算処理部142においてセキュアコンテナ104に関連したラインセンス 料の支払い額を決定する際に用いられる。

利用履歴データ108には、例えば、セキュアコンテナ104に格納されたコンテンツデータCの識別子Content\_ID、セキュアコンテナ104を配給したコンテンツプロバイダ101の識別子CP\_ID、セキュアコンテナ104を記録した記録は体の識別子Media\_ID、セキュアコンテナ104を配給を受けたSAM1051~1054の識別子SAM\_ID、当該SAM1051~1054のユ

ーザのUSER\_IDなどが記述されている。従って、EMDサービスセンタ102は、コンテンツプロバイダ101の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク103のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータ107および決済請求権データ152を作成する。当該分配率表は、例えば、セキュアコンテナ104に格納されたコンテンツデータ毎に作成される。

また、決済請求権データ152は、当該データに基づいて、決済機関91に金 銭の支払いを請求できる権威化されたデータであり、例えば、ユーザが支払った 金銭を複数の権利者に配給する場合には、個々の権利者毎に作成される。

なお、決済機関 9 1 は、決済が終了すると、当該決済機関の利用明細書をEMDサービスセンタ 1 0 2 に送る。EMDサービスセンタ 1 0 2 は、当該利用明細書の内容を、対応する権利者に通知する。

決算機関管理部144は、決算処理部142が生成した決済請求権利データ152を図1に示すペイメントゲートウェイ90を介して決済機関91に送信する

なお、後述するように、決算機関管理部144は、決済請求権データ152を 、コンテンツプロバイダ101などの権利者に送信し、権利者自らが、受信した 決済請求権データ152を用いて決済機関91に決済を行ってもよい。

また、決算機関管理部144は、署名処理部143において決済請求権データ 152のハッシュ値をとり、秘密鍵データKesc,s を用いて生成した署名データ SIGssを決済請求権データ152と共に決済機関91に送信する。

証明書・権利書管理部145は、CERデータベース145aに登録されて権 威化された公開鍵証明書データCER cpおよび公開鍵証明書データCER sami~ CER samiなどを読み出すと共に、コンテンツプロバイダ101の権利書データ 106およびコンテンツ鍵データKcなどをCERデータベース145aに登録

して権威化する。

なお、公開鍵証明書データCERsami~CERsamiを格納するデータベースと 、権利書データ 1 0 6 およびコンテンツ鍵データKcとを個別に設けてもよい。

このとき、証明書・権利書管理部 1 4 5 は、例えば、権利書データ 1 0 6 およびコンテンツ鍵データ K c などのハッシュ値をとり、秘密鍵データ K BSC. s を用いた署名データを付した権威化されたそれぞれの証明書データを作成する。

コンテンツプロバイダ管理部148は、コンテンツプロバイダ101との間で通信する機能を有し、登録されたコンテンツプロバイダ101の識別子CP\_IDなどを管理するCPデータベース148aにアクセスできる。

SAM管理部 149は、ユーザホームネットワーク 103内のSAM 1051~1054 との間で通信する機能を有し、登録されたSAMの識別子SAM\_IDやSAM登録リストなどを記録したSAMデータベース 149aにアクセスできる。

以下、EMDサービスセンタ102内での処理の流れを説明する。

先ず、EMDサービスセンタ102からコンテンツプロバイダ101およびユーザホームネットワーク103内のSAM1051~1054への配信用鍵データを送信する際の処理の流れを、図10および図11を参照しながら説明する。

図10に示すように、鍵サーバ141は、所定期間毎に、例えば、6カ月分の配信用鍵データKD1~KD8を鍵データベース141aから読み出してコンテンツプロバイダ管理部148に出力する。

また、署名処理部 143は、配信用鍵データ  $KD_1 \sim KD_6$  の各々のハッシュ値をとり、EMD サービスセンタ 102 の秘密鍵データ  $K_{BSC,S}$  を用いて、それぞれに対応する署名データ  $SIG_{KD1,BSC} \sim SIG_{KD6,BSC}$  を作成し、これをコンテンツプロバイダ管理部 148に出力する。

コンテンツプロバイダ管理部 148は、この 6 カ月分の配信用鍵データ K  $D_1$  ~ K  $D_8$  およびそれらの署名データ S I  $G_{KD1, BSC}$  ~ S I  $G_{KD8, BSC}$  を、相互認証部 150 と図 3 に示す相互認証部 120 と間の相互認証で得られたセッション鍵データ  $K_{SBS}$  を用いて暗号化した後に、コンテンツプロバイダ 101 に送信する。

また、図11に示すように、鍵サーバ141は、所定期間毎に、例えば、3カ月分の配信用鍵データ $KD_1 \sim KD_8$ を鍵データベース141 a から読み出してSAM管理部149に出力する。

SAM管理部 1 4 9 は、この 3 カ月分の配信用鍵データ  $KD_1 \sim KD_8$  および それらの署名データ  $SIG_{KD1, BSC} \sim SIG_{KD5, BSC}$  を、相互認証部 1 5 0 と  $SIG_{KD1, BSC} \sim 105$  と間の相互認証で得られたセッション鍵データ  $SIG_{KSB}$  を 用いて暗号化した後に、 $SIG_{KD1, BSC} \sim 105$  に送信する。

以下、EMDサービスセンタ102がコンテンツプロバイダ101から、公開 鍵証明書データCERcrの発行要求を受けた場合の処理を、図10および図12 を参照しながら説明する。

図12は、当該処理のフローチャートである。

ステップSC1:コンテンツプロバイダ管理部148は、コンテンツプロバイダ101の識別子CP\_ID、公開鍵データKcp.pおよび署名データSIGs.cpを含む公開鍵証明書データ発行要求をコンテンツプロバイダ101から受信すると、これらを、相互認証部150と図3に示す相互認証部120と間の相互認証で得られたセッション鍵データKsssを用いて復号する。

ステップSC2: 当該復号した署名データSIG೩ сгの正当性を署名処理部1

43において確認した後に、識別子CP\_IDおよび公開鍵データKcp.pに基づいて、当該公開鍵証明書データ発行要求を出したコンテンツプロバイダ101がCPデータベース148aに登録されているか否かを確認する。

ステップSC3:証明書・権利書管理部145は、当該コンテンツプロバイダ 101の公開鍵証明書データCERcrをCERデータベース145aから読み出 してコンテンツプロバイダ管理部148に出力する。

ステップSC4:署名処理部143は、公開鍵証明書データCERcpのハッシュ値をとり、EMDサービスセンタ102の秘密鍵データKBSC、Sを用いて、署名データSIG1.BSCを作成し、これをコンテンツプロバイダ管理部148に出力する。

ステップSC5:コンテンツプロバイダ管理部148は、公開鍵証明書データ CERcpおよびその署名データSIG1. BSC を、相互認証部150と図3に示す 相互認証部120と間の相互認証で得られたセッション鍵データKSBS を用いて 暗号化した後に、コンテンツプロバイダ101に送信する。

以下、EMDサービスセンタ102がSAM1051から、公開鍵証明書データCER<sub>SAM1</sub>の発行要求を受けた場合の処理を、図11および図13を参照しながら説明する。

図13は、当該処理のフローチャートである。

ステップSD1:SAM管理部149は、SAM105:の識別子SAM: — ID、公開鍵データKsami, pおよび署名データSIGs, samiを含む公開鍵証明書 データ発行要求をSAM105:から受信すると、これらを、相互認証部150とSAM105:と間の相互認証で得られたセッション鍵データKsss を用いて復号する。

ステップSD2: 当該復号した署名データSIG8, SAM1の正当性を署名処理部 143において確認した後に、識別子SAM1 \_ IDおよび公開鍵データK SAM1 \_ に基づいて、当該公開鍵証明書データの発行要求を出したSAM1051 がS

AMデータベース149aに登録されているか否かを確認する。

ステップSD3:証明書・権利書管理部145は、当該SAM1051の公開 鍵証明書データCER<sub>SAM1</sub>をCERデータベース145aから読み出してSAM 管理部149に出力する。

ステップSD4:署名処理部143は、公開鍵証明書データCERsamiのハッシュ値をとり、EMDサービスセンタ102の秘密鍵データKBSC.s を用いて、署名データSIG50.BSCを作成し、これをSAM管理部149に出力する。

ステップSD5:SAM管理部149は、公開鍵証明書データCERsam1およびその署名データSIG50. BScを、相互認証部150とSAM1051と間の相互認証で得られたセッション鍵データKSBSを用いて暗号化した後に、SAM1051に送信する。

なお、 $SAM1052\sim1054$ が、公開鍵証明書データを要求した場合の処理は、対象が $SAM1052\sim1054$ に代わるのみで、基本的に上述したSAM1051の場合と同じである。

なお、本発明では、EMDサービスセンタ102は、例えば、SAM1051の出荷時に、SAM1051の秘密鍵データ $K_{SAM1.S}$ および公開鍵データ $K_{SAM1.P}$ の記憶部に記憶する場合には、当該出荷時に、公開鍵データ $K_{SAM1.P}$ の公開鍵証明書データ $CER_{SAM1}$ を作成してもよい。

このとき、当該出荷時に、公開鍵証明書データCER<sub>SAM1</sub>を、SAM105<sub>1</sub>の記憶部に記憶してもよい。

以下、EMDサービスセンタ102が、コンテンツプロバイダ101から権利 書データ106およびコンテンツ鍵データKcの登録要求を受けた場合の処理を 、図10および図14を参照しながら説明する。

図14は、当該処理のフローチャートである。

ステップSE1:コンテンツプロバイダ管理部148は、コンテンツプロバイダ101から図7Aに示す権利書登録要求モジュールMod2を受信すると、相

互認証部150と図3に示す相互認証部120と間の相互認証で得られたセッション鍵データKses を用いて権利書登録要求モジュールMod2を復号する。

ステップSE2:署名処理部143において、鍵データベース141aから読み出した公開鍵データK。Fを用いて、署名データSIG5.cFの正当性を検証する。

ステップSE3:証明書・権利書管理部145は、権利書登録要求モジュール Mod2 に格納された権利書データ106およびコンテンツ鍵データKcを、CERデータベース145aに登録する。

以下、EMDサービスセンタ102において決済処理を行なう場合の処理を図11および図15を参照しながら説明する。

図15は、当該処理のフローチャートである。

ステップSF1:SAM管理部149は、ユーザホームネットワーク103の例えばSAM1051から利用履歴データ108およびその署名データSIG200. SAM1を入力すると、利用履歴データ108および署名データSIG200. SAM1を、相互認証部150とSAM1051との間の相互認証によって得られたセッション鍵データKSBSを用いて復号し、SAM1051の公開鍵データKSAM1による署名データSIG200. SAM1の検証を行なった後に、決算処理部142に出力する。

ステップSF2:決算処理部142は、SAM管理部149から入力した利用履歴データ108と、証明書・権利書管理部145を介してCERデータベース145aから読み出した権利書データ106に含まれる標準小売価格データSRPおよび販売価格とに基づいて決済処理を行い、決済請求権データ152および決済レポートデータ107を生成する。なお、決済請求権データ152および決済レポートデータ107の生成は、SAMから利用履歴データ108を入力する度に行ってもよいし、所定の期間毎に行ってもよい。

ステップSF3:決算処理部142は、決済請求権データ152を決算機関管

理部144に出力する。

決算機関管理部144は、決済請求権データ152およびその署名データSIG<sub>88</sub>を、相互認証およびセッション鍵データK<sub>SBS</sub> による復号を行なった後に、図1に示すペイメントゲートウェイ90を介して決済機関91に送信する。

これにより、決済請求権データ152に示される金額の金銭が、コンテンツプロバイダ101に支払われる。

なお、EMDサービスセンタ102は、決済請求権データ152をコンテンツ プロバイダ101に送信し、コンテンツプロバイダ101が決済請求権データ1 52を用いて決済記載91に金銭を請求してもよい。

ステップSF4:決算処理部142は、決済レポートデータ107をコンテンツプロバイダ管理部148に出力する。

決済レポートデータ107は、上述したように、例えば、EMDサービスセンタ102が図1に示す決済機関91に対して行なったコンテンツプロバイダ101に関する決済の内容が記述されている。

コンテンツプロバイダ管理部148は、決済レポートデータ107を、相互認証部150と図3に示す相互認証部120と間の相互認証で得られたセッション鍵データKses を用いて暗号化した後に、コンテンツプロバイダ101に送信する。

また、EMDサービスセンタ 102は、前述したように、権利書データ 106を登録(権威化)した後に、EMDサービスセンタ 102からコンテンツプロバイダ 101に、図 7Bに示す権威化証明書モジュールM  $od_2$  a を配信用鍵データ  $KD_1 \sim KD_8$  で暗号化して送信してもよい。

また、EMDサービスセンタ102は、その他に、 $SAM105_1 \sim 105_4$ の出荷時の処理と、SAM登録リストの登録処理とを行なうが、これらの処理については後述する。

[ユーザホームネットワーク103]

ューザホームネットワーク 103 は、図 1 に示すように、ネットワーク機器 160 な を有している。

ネットワーク機器 1601 は、SAM1051 を内蔵している。また、AV機器 1602 ~ 1604 は、それぞれSAM1052 ~ 1054 を内蔵している。

 $SAM1051 \sim 1054$  の相互間は、例えば、IEEE1394 シリアルインタフェースバスなどのバス191を介して接続されている。

なお、AV機器1602~160.は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス191を介してネットワーク機器160.のネットワーク通信機能を利用してもよい。

また、ユーザホームネットワーク103は、ネットワーク機能を有していない AV機器のみを有していてもよい。

以下、ネットワーク機器1601について説明する。

図16ネットワーク機器1601の構成図である。

図16に示すように、ネットワーク機器1601は、SAM1051、通信モジュール162、復号・伸長モジュール163、購入・利用形態決定操作部165、ダウンロードメモリ167、再生モジュール169および外部メモリ201を有する。

 $SAM1051 \sim 1051$ は、コンテンツ単位の課金処理をおこなうモジュールであり、EMDサービスセンタ102との間で通信を行う。

SAM1051~1051は、例えば、EMDサービスセンタ102によって 仕様およびバージョンなどが管理され、家庭機器メーカに対し、搭載の希望があればコンテンツ単位の課金を行うプラックボックスの課金モジュールとしてライセンス譲渡される。例えば、家庭機器開発メーカは、SAM1051~1051 のIC(Integrated Circuit)の内部の仕様を知ることはできず、EMDサービスセンタ102が当該ICのインタフェースなどを統一化し、それに従ってネット

ワーク機器 1 6 0 1 および A V 機器 1 6 0 2 ~ 1 6 0 a に搭載される。

 $SAM1051\sim105$ 。は、その処理内容が外部から完全に遮蔽され、その処理内容を外部から監視および改竄不能であり、また、内部に予め記憶されているデータおよび処理中のデータを外部から監視および改竄不能な耐タンパ(Tamper Registance)性を持ったハードウェアモジュール(ICモジュールなど)である。

SAM1051~105.の機能をICという形で実現する場合は、IC内部に秘密メモリを持ち、そこに秘密プログラムおよび秘密データが格納される。SAMをICという物理的形態にとらわれず、その機能を機器の何れかの部分に組み込むことができれば、その部分をSAMとして定義してもよい。

以下、SAM105」の機能について詳細に説明する。

なお、SAM1052~1054は、SAM1051と基本的に同じ機能を有 している。

図17は、SAM1051の機能の構成図である。

なお、図17には、コンテンツプロバイダ101からのセキュアコンテナ10 4を入力し、セキュアコンテナ104内のキーファイルKFを復号する処理に関 連するデータの流れが示されている。

図17に示すように、SAM1051は、相互認証部170、暗号化・復号部171,172,173、コンテンツプロバイダ管理部180、誤り訂正部181、ダウンロードメモリ管理部182、セキュアコンテナ復号部183、復号・伸長モジュール管理部184、EMDサービスセンタ管理部185、利用監視部186、課金処理部187、署名処理部189、SAM管理部190、メディアSAM管理部197、スタック(作業)メモリ200および外部メモリ管理部81を有する。

なお、AV機器 $160_2 \sim 160$ 、はダウンロードメモリ167を有していないため、SAM $105_2 \sim 105$ 。にはダウンロードメモリ管理部182は存在

しない。

なお、図17に示すSAM105:の所定の機能は、例えば、図示しないCP IIにおいて秘密プログラムを実行することによって実現される。

また、スタックメモリ200には、以下に示す処理を経て、図18に示すように、利用履歴データ108およびSAM登録リストが記憶される。

ここで、外部メモリ201のメモリ空間は、SAM1051の外部(例えば、ホストCPU810)からは見ることはできず、SAM1051のみが外部メモリ201の記憶領域に対してのアクセスを管理できる。

外部メモリ201としては、例えば、フラッシュメモリあるいは強誘電体メモリ(FeRAM)などが用いられる。

また、スタックメモリ200としては、例えばSARAMが用いられ、図19に示すように、セキュアコンテナ104、コンテンツ鍵データKc、権利書データ(UCP)106、記憶部192のロック鍵データKLoc 、コンテンツプロバイダ101の公開鍵証明書 $CER_{CP}$ 、利用制御状態データ(UCS)166、およびSAMプログラム・ダウンロード・コンテナSDC1 ~SDC8 などが記憶される。

以下、SAM1051の機能のうち、コンテンツプロバイダ101からのセキュアコンテナ104を入力したときの各機能プロックの処理内容を図17を参照しながら説明する。

相互認証部170は、SAM1051がコンテンツプロバイダ101およびEMDサービスセンタ102との間でオンラインでデータを送受信する際に、コンテンツプロバイダ101およびEMDサービスセンタ102との間で相互認証を行ってセッション鍵データ(共有鍵) $K_{SBS}$ を生成し、これを暗号化・復号部171に出力する。セッション鍵データ $K_{SBS}$ は、相互認証を行う度に新たに生成される。

暗号化・復号部171は、コンテンツプロバイダ101およびEMDサービス

センタ102との間で送受信するデータを、相互認証部170が生成したセッション鍵データKsgs を用いて暗号化・復号する。

誤り訂正部181は、セキュアコンテナ104を誤り訂正してダウンロードメモリ管理部182に出力する。

なお、ユーザホームネットワーク103は、セキュアコンテナ104が改竄されているか否かを検出する機能を有していてもよい。

本実施形態では、誤り訂正部 1 8 1 を、SAM 1 0 5 1 に内蔵した場合を例示したが、誤り訂正部 1 8 1 の機能を、例えばホスト CP U 8 1 0 などの SAM 1 0 5 1 の外部に持たせてもよい。

ダウンロードメモリ管理部182は、図16に示すようにダウンロードメモリ167が相互認証機能を持つメディアSAM167aを有している場合には、相互認証部170とメディアSAM167aとの間で相互認証を行った後に、誤り訂正後のセキュアコンテナ104を、相互認証によって得られたセッション鍵データKsBs を用いて暗号化して図16に示すダウンロードメモリ167に書き込む。ダウンロードメモリ167としては、例えば、メモリスティックなどの不揮発性半導体メモリが用いられる。

なお、図20に示すように、HDD(Hard Disk Drive)などの相互認証機能を備えていないメモリをダウンロードメモリ211として用いる場合には、ダウンロードメモリ211内はセキュアではないので、コンテンツファイルCFをダウンロードメモリ211にダウンロードし、機密性の高いキーファイルKFを例えば、図17に示すスタックメモリ200にダウンロードする。

セキュアコンテナ復号部183は、ダウンロードメモリ管理部182から入力したセキュアコンテナ104に格納されたキーファイルKFを、記憶部192から読み出した対応する期間の配信用鍵データKD1 $\sim$ KD8を用いて復号し、署名処理部189において署名データSIG2.cF $\sim$ SIG4.cF $\sigma$ D5 でなわちコンテンツデータC、コンテンツ鍵データKcおよび権利書データ106の作成

者の正当性を確認した後に、スタックメモリ200に書き込む。

EMDサービスセンタ管理部185は、図1に示すEMDサービスセンタ102との間の通信を管理する。

署名処理部189は、記憶部192から読み出したEMDサービスセンタ10 2の公開鍵データK<sub>BSC, P</sub> およびコンテンツプロバイダ101の公開鍵データK<sub>CP, P</sub>を用いて、セキュアコンテナ104内の署名データの検証を行なう。

記憶部192は、SAM1051の外部から読み出しおよび書き換えできない秘密データとして、図21に示すように、配信用鍵データKD1~KDs、SAM\_ID、ユーザID、パスワード、情報参照用ID、SAM登録リスト、記録用鍵データKstr、ルートCAの公開鍵データKr-ca.p、EMDサービスセンタ102の公開鍵データKbsc.p、メディア鍵データKmbd、EMDサービスセンタ102の公開鍵データKbsc.p、SAM1051の秘密鍵データKsam1.s、SAM1051の公開鍵データKsam1.pを格納した公開鍵証明書CERsam1、EMDサービスセンタ102の秘密鍵データKsam1.pを格納した公開鍵証明書CERsam1、EMDサービスセンタ102の秘密鍵データKbsc.sを用いた公開鍵証明書CERbscの署名データSIG22、復号・伸長モジュール163との間の相互認証用の元鍵データを記憶している。

また、記憶部192には、図17に示す少なくとも一部の機能を実現するための秘密プログラムが記憶されている。

記憶部192としては、例えば、フラッシューEEPROM(Electrically Erasable Programmable RAM)が用いられる。

以下、SAM1051の処理の流れのうち、コンテンツプロバイダ101からのセキュアコンテナ104を入力したときの処理の流れを説明する。

先ず、EMDサービスセンタ 102 から受信した配信用鍵データ  $KD_1 \sim KD_2$  。を記憶部 192 に格納する際のSAM1051 内での処理の流れを図 17 を参照しながら説明する。

この場合には、先ず、相互認証部170と図10に示す相互認証部150との

間で相互認証が行われる。

次に、当該相互認証によって得られたセッション鍵データ $K_{SBS}$  で暗号化された 3 カ月分の配信用鍵データ $K_{D1}$  ~ $K_{DS}$  およびその署名データ $S_{IG_{KD1,BS}}$  c ~ $S_{IG_{KDS,BSC}}$  が、 $E_{MD}$  サービスセンタ 1 0 2 から $E_{MD}$  サービスセンタ 管理部 1 8 5 を介してスタックメモリ 8 1 1 に書き込まれる。

次に、暗号化・復号部171において、セッション鍵データ $K_{SBS}$  を用いて、配信用鍵データ $KD_1 \sim KD_8$  およびその署名データ $SIG_{KD1,BSC} \sim SIG_{KD}$ 8. BSC が復号される。

次に、署名処理部 189 において、スタックメモリ 811 に記憶された署名データ  $SIG_{KD1, BSC} \sim SIG_{KDS, BSC}$  の正当性が確認された後に、配信用鍵データ  $KD_1 \sim KD_3$  が記憶部 192 に書き込まれる。

以下、セキュアコンテナ104をコンテンツプロバイダ101から入力し、セキュアコンテナ104内のキーファイルKFを復号する際のSAM1051内での処理の流れを図17および図22を参照しながら説明する。

図22は、当該処理のフローチャートである。

ステップSG1:図17に示すSAM1051の相互認証部170と図2に示す相互認証部120との間で相互認証が行なわれる。

暗号化・復号部171は、当該相互認証によって得られたセッション鍵データ Kses を用いて、コンテンツプロバイダ管理部180を介してコンテンツプロバイダ101から受信したセキュアコンテナ104を復号する。

ステップSG 2:署名処理部 189は、図4Cに示す署名データSIG 1. BSC の検証を行なった後に、図4Cに示す公開鍵証明書データCER  $_{cP}$ 内に格納されたコンテンツプロバイダ 101の公開鍵データ $_{KcP,P}$ を用いて、署名データSIG  $_{6,CP}$ , SIG  $_{7,CP}$ の正当性を確認する。

コンテンツプロバイダ管理部180は、署名データSIG\*, cp, SIG\*, cpの 正当性が確認されると、セキュアコンテナ104を誤り訂正部181に出力する

誤り訂正部181は、セキュアコンテナ104を誤り訂正した後に、ダウンロードメモリ管理部182に出力する。

ステップSG3:ダウンロードメモリ管理部182は、相互認証部170と図 16に示すメディアSAM167aとの間で相互認証を行なった後に、セキュア コンテナ104をダウンロードメモリ167に書き込む。

ステップSG4:ダウンロードメモリ管理部182は、相互認証部170と図16に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ104に格納された図4Bに示すキーファイルKFをダウンロードメモリ167から読み出してセキュアコンテナ復号部183に出力する。

そして、セキュアコンテナ復号部183は、記憶部192から入力した対応する期間の配信用鍵データKD1~KD8を用いて、キーファイルKFを復号し、図4Bに示す署名・証明書モジュールMod1に格納された署名データSIG1. BSC、SIG2. CP~SIG4. CPを署名処理部189に出力する。

ステップSG 5:署名処理部 189は、図 4Bに示す署名データS  $IG_{1.BSC}$ の検証を行なった後に、図 4Bに示す公開鍵証明書データC  $ER_{CP}$ 内に格納された公開鍵データ $K_{BSC,P}$ を用いて署名データS  $IG_{2.CP}$ ~S  $IG_{4.CP}$ の検証を行なう。これにより、コンテンツデータC、コンテンツ鍵データ $K_{C}$  および権利書データ 106 の作成者の正当性が検証される。

ステップSG 6:セキュアコンテナ復号部183は、署名データSIG2.  $c_P \sim SIG_4$ .  $c_P \circ O$  正当性が確認されると、キーファイルKFをスタックメモリ200 に書き込む。

以下、ダウンロードメモリ167にダウンロードされたコンテンツデータCを 利用・購入する処理に関連する各機能プロックの処理内容を図23を参照しなが ら説明する。

利用監視部186は、スタックメモリ200から権利書データ106および利

用制御状態データ166を読み出し、当該読み出した権利書データ106および 利用制御状態データ166によって許諾された範囲内でコンテンツの購入・利用 が行われるように監視する。

ここで、権利書データ106は、図17を用いて説明したように、復号後にスタックメモリ200に記憶された図4Bに示すキーファイルKF内に格納されている。

また、利用制御状態データ166は、後述するように、ユーザによって購入形態が決定されたときに、スタックメモリ200に記憶される。

課金処理部187は、図16に示す購入・利用形態決定操作部165からの操作信号S165に応じた利用履歴データ108を作成する。

ここで、利用履歴データ108は、前述したように、ユーザによるセキュアコンテナ104の購入および利用の形態の履歴を記述しており、EMDサービスセンタ102において、セキュアコンテナ104の購入に応じた決済処理およびラインセンス料の支払いを決定する際に用いられる。

また、課金処理部187は、必要に応じて、スタックメモリ200から読み出した販売価格あるいは標準小売価格データSRPをユーザに通知する。

ここで、販売価格および標準小売価格データSRPは、復号後にスタックメモリ200に記憶された図4Bに示すキーファイルKFの権利書データ106内に格納されている。

課金処理部187による課金処理は、利用監視部186の監視の下、権利書データ106が示す使用許諾条件などの権利内容および利用制御状態データ166に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行う。

また、課金処理部187は、操作信号S165に基づいて、ユーザによるコンテンツの購入形態を記述した利用制御状態 (UCS: Usage Control Status)データ166を生成し、これをスタックメモリ200に書き込む。

コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。

ここで、利用制御状態データ166は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御状態データ166には、コンテンツのID、購入形態、当該購入形態に応じた価格、当該コンテンツの購入が行なわれたSAMのSAM\_ID,購入を行なったユーザのUSER\_IDなどが記述されている。

なお、決定された購入形態が再生課金である場合には、例えば、SAM105 1 からコンテンツプロバイダ101に利用制御状態データ166をコンテンツデータCの購入と同時にリアルタイムに送信し、コンテンツプロバイダ101がEMDサービスセンタ102に、利用履歴データ108を所定の期間内にSAM1051に取りにいくことを指示する。

また、決定された購入形態が買い切りである場合には、例えば、利用制御状態 データ166が、コンテンツプロバイダ101およびEMDサービスセンタ10 2の双方にリアルタイムに送信される。このように、本実施形態では、何れの場 合にも、利用制御状態データ166をコンテンツプロバイダ101にリアルタイムに送信する。

EMDサービスセンタ管理部185は、外部メモリ管理部811を介して外部メモリ201から読み出した利用履歴データ108をEMDサービスセンタ102に送信する。

このとき、EMDサービスセンタ管理部185は、署名処理部189において、秘密鍵データK<sub>SAM1</sub>、を用いて利用履歴データ108の署名データSIG<sub>200</sub>、<sub>SAM1</sub>を作成し、署名データSIG<sub>200</sub>、<sub>SAM1</sub>を利用履歴データ108と共にEMDサービスセンタ102に送信する。

EMDサービスセンタ102への利用履歴データ108の送信は、例えば、EMDサービスセンタ102からの要求に応じてあるいは定期的に行ってもよいし、利用履歴データ108に含まれる履歴情報の情報量が所定以上になったときに行ってもよい。当該情報量は、例えば、外部メモリ201の記憶容量に応じて決定される。

ダウンロードメモリ管理部182は、例えば、図16に示す購入形態決定操作部165からの操作信号S165に応じてコンテンツの再生動作が行われる場合に、ダウンロードメモリ167から読み出したコンテンツデータC、スタックメモリ200から読み出したコンテンツ鍵データKcおよび課金処理部187から入力したユーザ電子透かし情報用データ186を復号・伸長モジュール管理部184に出力する。

また、復号・伸長モジュール管理部184は、図16に示す購入形態決定操作部165からの操作信号S165に応じてコンテンツの試聴動作が行われる場合に、ダウンロードメモリ167から読み出したコンテンツファイルCF、並びにスタックメモリ200から読み出したコンテンツ鍵データKcおよび半開示パラメータデータ189を復号・伸長モジュール管理部184に出力する。

ここで、半開示パラメータデータ199は、権利書データ106内に記述されており、試聴モード時のコンテンツの取り扱いを示している。復号・伸長モジュール163では、半開示パラメータデータ199に基づいて、暗号化されたコンテンツデータCを、半開示状態で再生することが可能になる。半開示の手法としては、例えば、復号・伸長モジュール163がデータ(信号)を所定のブロックを単位として処理することを利用して、半開示パラメータデータ199によって、コンテンツ鍵データKcを用いて復号を行うプロックと復号を行わないプロックとを指定したり、試聴時の再生機能を限定したり、試聴可能な期間を限定するものなどがある。

以下、SAM1051内での処理の流れについて説明する。

先ず、コンテンツプロバイダ101からダウンロードメモリ167にダウンロードされたセキュアコンテナ104の購入形態を決定するまでの処理の流れを図23および図24を参照しながら説明する。

図24は、当該処理のフローチャートである。

ステップSH1:課金処理部187において、ユーザによる図16に示す購入
・利用形態決定操作部165の操作によって、試聴モードを示す操作信号S16
5が発生したか否かが判断され、発生したと判断された場合にはステップSH2
の処理が行われ、そうでない場合にはステップSH3の処理が行われる。

ステップSH2:課金処理部187によって、例えば、ダウンロードメモリ167に記憶されているコンテンツファイルCFが、復号・伸長モジュール管理部184を介して、図16に示す復号・伸長モジュール163に出力される。

このとき、コンテンツファイルCFに対して、相互認証部170とメディアSAM167aとの間の相互認証およびセッション鍵データKses による暗号化・復号と、相互認証部170と相互認証部220との間の相互認証およびセッション鍵データKses による暗号化・復号とが行なわれる。

コンテンツファイルCFは、図16に示す復号部221において復号された後に、復号部222に出力される。

また、スタックメモリ200から読み出されたコンテンツ鍵データKcおよび 半開示パラメータデータ199が、図16に示す復号・伸長モジュール163に 出力される。このとき、相互認証部170と相互認証部220との間の相互認証 後に、コンテンツ鍵データKcおよび半開示パラメータデータ199に対してセ ッション鍵データKsss による暗号化および復号が行なわれる。

次に、復号された半開示パラメータデータ199が半開示処理部225に出力され、半開示処理部225からの制御によって、復号部222によるコンテンツ鍵データKcを用いたコンテンツデータCの復号が半開示で行われる。

次に、半開示で復号されたコンテンツデータCが、伸長部223において伸長

された後に、電子透かし情報処理部224に出力される。

次に、電子透かし情報処理部224においてユーザ電子透かし情報用データ186がコンテンツデータCに埋め込まれた後、コンテンツデータCが再生モジュール169において再生され、コンテンツデータCに応じた音響が出力される。ステップSH3:ユーザが購入・利用形態決定操作部165を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号S165が課金処理部187に出力される。

ステップSH4:課金処理部187において、決定された購入形態に応じた利用履歴データ108および利用制御状態データ166が生成され、利用履歴データ108が外部メモリ管理部811を介して外部メモリ201に書き込まれると共に、利用制御状態データ166がスタックメモリ200に書き込まれる。

以後は、利用監視部186において、利用制御状態データ166によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御(監視)される。

ステップSH5:スタックメモリ200に格納されているキーファイルKFに、利用制御状態データ166が加えられ、購入形態が決定した後述する図29Bに示す新たなキーファイルKF:が生成される。キーファイルKF:は、スタックメモリ200に記憶される。

図29Bに示すように、キーファイル $KF_1$  に格納された利用制御状態データ 166 はストレージ鍵データ $K_{STR}$  を用いてDESのCBCモードを利用して暗号化されている。また、当該ストレージ鍵データ $K_{STR}$  をMAC鍵データとして用いて生成したMAC値であるMACsoo が付されている。また、利用制御状態データ 166 およびMACsoo からなるモジュールは、メディア鍵データ $K_{MED}$  を用いてDESのCBCモードを利用して暗号化されている。また、当該モジュールには、当該メディア鍵データ $K_{MED}$  をMAC鍵データとして用いて生成したMAC値であるMACso1 が付されている。

以下、ダウンロードメモリ167に記憶されている購入形態が既に決定された コンテンツデータCを再生する場合の処理の流れを、図23および図25を参照 しながら説明する。

図25は、当該処理のフローチャートである。

ステップSI1:課金処理部187が、ユーザによる操作に応じて、再生を行うコンテンツを指定した操作信号S165を入力する。

ステップSI2:課金処理部187は、利用監視部186の監視下で、操作信号S165に基づいて、ダウンロードメモリ167に記憶されているコンテンツファイルCFが読み出される。

ステップSI3:当該読み出されたコンテンツファイルCFが図16に示す復号・伸長モジュール163に出力される。このとき、図23に示す相互認証部170と、図16に示す復号・伸長モジュール163の相互認証部220との間で相互認証が行われる。

また、スタックメモリ200から読み出されたコンテンツ鍵データKcが復号・伸長モジュール163に出力される。

ステップSI4:復号・伸長モジュール163の復号部222において、コンテンツ鍵データKcを用いたコンテンツファイルCFの復号と、伸長部223による伸長処理とが行なわれ、再生モジュール169において、コンテンツデータ Cが再生される。

ステップSI5:課金処理部187によって、操作信号S165に応じて、外部メモリ201に記憶されている利用履歴データ108が更新される。

利用履歴データ108は、外部メモリ201から読み出された後、相互認証を経て、EMDサービスセンタ管理部185を介して、署名データSIG200. SAM1と共にEMDサービスセンタ102に送信される。

以下、図26に示すように、例えば、ネットワーク機器1601のダウンロードメモリ167にダウンロードされた既に購入形態が決定されたコンテンツファ

イルCFおよびキーファイルKFを、バス191を介して、AV機器160 $_2$ のSAM105 $_2$ に転送する場合のSAM105 $_1$ 内での処理の流れを図27および図28を参照しながら説明する。

図28は、当該処理のフローチャートである。

ステップS J 1: ユーザは、購入・利用形態決定操作部 1 6 5 を操作して、ダウンロードメモリ 1 6 7 に記憶された所定のコンテンツをA V 機器 1 6 0 2 に転送することを指示し、当該操作に応じた操作信号S 1 6 5 が、課金処理部 1 8 7 に出力される。

これにより、課金処理部187は、操作信号S165に基づいて、外部メモリ201に記憶されている利用履歴データ108を更新する。

ステップSJ2:ダウンロードメモリ管理部182は、ダウンロードメモリ167から読み出した図29Aに示すコンテンツファイルCFをSAM管理部190に出力する。

ステップSJ3:スタックメモリ200から読み出した図29Bに示すキーファイルKF1を、署名処理部189およびSAM管理部190に出力する。

ステップS J 4:署名処理部 189は、スタックメモリ 200から読み出した キーファイル $KF_1$  の署名データS  $IG_{42.SAM1}$  を作成し、これをSAM管理部 190に出力する。

また、SAM管理部190は、記憶部192から、図29Cに示す公開鍵証明 書データCER<sub>SAM1</sub>およびその署名データSIG<sub>22. BSC</sub>を読み出す。

ステップSJ5:相互認証部170は、SAM1052 との間で相互認証を行って得たセッション鍵データKsBs を暗号化・復号部171に出力する。

SAM管理部190は、図29A、図29B、図29Cに示すデータからなる新たなセキュアコンテナを作成する。

ステップSJ6:暗号化・復号部171において、セッション鍵データKsBs を用いて暗号化した後に、図26に示すAV機器1602のSAM1052に出

力する。

このとき、SAM1051 とSAM1052 との間の相互認証と並行して、IEEE1394シリアルバスであるバス191の相互認証が行われる。

以下、図26に示すように、SAM1051 から入力したコンテンツファイル CFなどを、RAM型などの記録媒体(メディア)に書き込む際のSAM1052 内での処理の流れを、図30および図31を参照しながら説明する。

図31は、当該処理のフローチャートである。

ステップSK1:SAM1052のSAM管理部190は、図26に示すように、図29Aに示すコンテンツファイルCFと、図29Bに示すキーファイルKF1 およびその署名データSIG42. SAM1 と、図29Cに示す公開鍵署名データCERSAM1およびその署名データSIG22. BSCとを、ネットワーク機器1601のSAM1051から入力する。

そして、暗号化・復号部171において、SAM管理部190が入力したコンテンツファイルCFと、キーファイルKF1 およびその署名データSIG42. SAM1 と、公開鍵署名データCER SAM1およびその署名データSIG22. BSCとが、相互認証部170とSAM1051 の相互認証部170との間の相互認証によって得られたセッション鍵データKSBS を用いて復号される。

次に、セッション鍵データ $K_{SBS}$  を用いて復号されたキーファイル $KF_1$  およびその署名データ $SIG_{22,BSC}$ とが、スタックメモリ200に書き込まれる。

ステップSK2:署名処理部189は、スタックメモリ200から読み出した 署名データSIG<sub>22. BSC</sub>を、記憶部192から読み出した公開鍵データK<sub>BSC. P</sub>を用いて検証して、公開鍵証明書データCER<sub>SAM1</sub>の正当性を確認する。

そして、署名処理部189は、公開鍵証明書データCERsam1の正当性を確認すると、公開鍵証明書データCERsam1に格納された公開鍵データKsam1.pを用いて、署名データSIG42.sam1 の正当を確認する。

次に、署名データSIG42、SAM1 の正当性、すなわちキーファイルKF1 の作成者の正当性が確認されると、図29Bに示すキーファイルKF1 をスタックメモリ200から読み出して暗号化・復号部173に出力する。

なお、当該例では、キーファイルKF1の作成者と送信元とが同じ場合を述べたが、キーファイルKF1の作成者と送信元とが異なる場合には、キーファイルKF1に対して作成者の署名データと送信者と署名データとが作成され、署名処理部189において、双方の署名データの正当性が検証される。

ステップSK3:暗号化・復号部173は、記憶部192から読み出した記録用鍵データ $K_{STR}$ 、メディア鍵データ $K_{MBD}$  および購入者鍵データ $K_{PIN}$  を用いてキーファイル $KF_1$  を順に暗号化してメディアSAM管理部197に出力する

なお、メディア鍵データ $K_{MBD}$ は、図27に示す相互認証部170と図26に示すRAM型の記録媒体250のメディアSAM252との間の相互認証によって記憶部192に事前に記憶されている。

ここで、記録用鍵データ $K_{STR}$  は、例えばSACD(Super Audio Compact Dis c)、DVD(Digital Versatile Disc)機器、CD-R機器およびMD(Mini Disc) 機器などの種類(当該例では、AV機器  $160_2$ )に応じて決まるデータであり、機器の種類と記録媒体の種類とを 1 対 1 で対応づけるために用いられる。なお、SACDEDVDEでは、ディスク媒体の物理的な構造が同じであるため、DVD機器を用いてSACDの記録媒体の記録・再生を行うことができる場合がある。記録用鍵データ $K_{STR}$  は、このような場合において、不正コピーを防止する役割を果たす。

また、メディア鍵データ $K_{MBD}$  は、記録媒体(当該例では、RAM型の記録媒体 (45.0) にユニークなデータである。

メディア鍵データ $K_{MED}$  は、記録媒体(当該例では、図26に示すRAM型の記録媒体 250)側に格納されており、記録媒体のメディアSAMにおいてメデ

ィア鍵データ Киво を用いた暗号化および復号を行うことがセキュリティの観点から好ましい。このとき、メディア鍵データ Киво は、記録媒体にメディアS A Mが搭載されている場合には、当該メディアS A M内に記憶されており、記録媒体にメディアS A Mが搭載されていない場合には、例えば、R A M領域内のホスト C P U 8 1 0 の管理外の領域に記憶されている。

なお、本実施形態のように、機器側のSAM(当該例では、 $SAM105_2$ )とメディアSAM(当該例では、メディアSAM252)との間で相互認証を行い、セキュアな通信経路を介してメディア鍵データ $K_{MBD}$ を機器側のSAMに転送し、機器側のSAMにおいてメディア鍵データ $K_{MBD}$ を用いた暗号化および復号を行なってもよい。

本実施形態では、記録用鍵データK<sub>STR</sub> およびメディア鍵データK<sub>MBD</sub> が、記録媒体の物理層のレベルのセキュリティを保護するために用いられる。

また、購入者鍵データ $K_{PIN}$ は、コンテンツファイルCFの購入者を示すデータであり、例えば、コンテンツを買い切りで購入したときに、当該購入したユーザに対してEMDサービスセンタ102によって割り当てられる。購入者鍵データ $K_{PIN}$ は、EMDサービスセンタ102において管理される。

ステップSK4:メディアSAM管理部197は、SAM管理部190から入力したコンテンツファイルCFおよび暗号化・復号部173から入力したキーファイルKF1を、図26に示す記録モジュール260に出力する。

そして、記録モジュール260は、メディアSAM管理部197から入力した コンテンツファイルCFおよびキーファイルKF1を、図26に示すRAM型の 記録媒体250のRAM領域251に書き込む。この場合に、キーファイルKF 1を、メディアSAM252内に書き込むようにしてもよい。

以下、コンテンツの購入形態が未決定の図6に示すROM型の記録媒体130 をユーザホームネットワーク303がオフラインで配給を受けた場合に、AV機 器1602において購入形態を決定する際の処理の流れを図32、図33、図3

4、図35を参照しながら説明する。

ステップSL1:AV機器1602のSAM1052は、先ず、図33に示す相互認証部170と図6に示すROM型の記録媒体130のメディアSAM133との間で相互認証を行った後に、メディアSAM133からメディア鍵データ Kmed を入力する。

なお、SAM1052が、事前にメディア鍵データKMBD を保持している場合には、当該入力を行わなくても良い。

ステップSL2:ROM型の記録媒体130のRAM領域132に記録されているセキュアコンテナ104に格納された図4B、Cに示すキーファイルKFおよびその署名データSIG7、 $c_P$ と、公開鍵証明書データCER $c_P$ およびその署名データSIG1、BSCとが、メディアSAM管理部197を介して入力され、これらがスタックメモリ200に書き込まれる。

ステップSL3:署名処理部189において、署名データSIG1、BSC の正当性を確認した後に、公開鍵証明書データCER $c_P$ から公開鍵データ $K_{c_P, P}$ を取り出し、この公開鍵データ $K_{c_P, P}$ を用いて、署名データSI $G_{7, c_P}$ の正当性、すなわちキーファイルKFの作成者の正当性を検証する。

ステップSL4:署名処理部189において署名データSIG7.cpの正当性が確認されると、スタックメモリ200からセキュアコンテナ復号部183に、キーファイルKFを読み出す。

そして、セキュアコンテナ復号部183において、対応する期間の配信用鍵データKD1~KDsを用いて、キーファイルKFを復号する。

ステップSL5:署名処理部189において、公開鍵データ $K_{BSC,P}$ を用いて、キーファイルKFに格納された署名データSI $G_{1,BSCM}$ の正当性を確認した後に、キーファイルKF内の公開鍵証明書データ $CER_{CP}$ に格納された公開鍵データ $K_{CP,P}$ を用いて、署名データSI $G_{2,CP}$ ~SI $G_{4,CP}$ の正当性、すなわちコンテンツデータC、コンテンツ鍵データ $K_{C}$ および権利書データ106の作成者の

正当性を検証する。

ステップSL6: 課金処理部187において、ユーザによる図16に示す購入・利用形態決定操作部165の操作によって、試聴モードを示す操作信号S165が発生したか否かが判断され、発生したと判断された場合にはステップSL7の処理が行われ、そうでない場合にはステップSL8の処理が行われる。

ステップSL7:図33に示す相互認証部170と図32に示す復号・伸長モジュール163との間で相互認証を行った後に、SAM1052の復号・伸長モジュール管理部184は、スタックメモリ200に記憶されているコンテンツ鍵データKcおよび権利書データ106に格納された半開示パラメータデータ193、並びにROM型の記録媒体130のROM領域131から読み出したコンテンツデータCを図32に示す復号・伸長モジュール163に出力する。次に、復号・伸長モジュール163において、コンテンツデータCがコンテンツ鍵データKcを用いて半開示モードで復号された後に伸長され、再生モジュール270に出力される。そして、再生モジュール270において、復号・伸長モジュール163からのコンテンツデータCが試聴モードで再生される。

ステップSL8:ユーザによる図32に示す購入形態決定操作部165の購入 操作によってコンテンツの購入形態が決定され、当該決定された購入形態を示す 操作信号S165が課金処理部187に入力される。

ステップSL9:課金処理部187は、操作信号S165に応じた利用制御状態データ166を作成し、これをスタックメモリ200に書き込む。

また、課金処理部187は、利用履歴データ108を作成あるいは更新する。

ステップSL10:スタックメモリ200から暗号化・復号部173に、例えば、図4Bに示すキーファイルKFに利御制御状態データ166を格納した図29Bに示す新たなキーファイルKF1が出力される。

ステップSL11:暗号化・復号部173は、スタックメモリ200から読み

出した図29Bに示すキーファイル $KF_1$ を、記憶部192から読み出した記録用鍵データ $K_{STR}$ 、メディア鍵データ $K_{MBD}$  および購入者鍵データ $K_{PIN}$ を用いて順次に暗号化してメディアSAM管理部197に出力する。

ステップSL12:図33に示す相互認証部170と図32に示すメディアSAM133との間で相互認証を行った後に、SAM管理部197は、暗号化・復号部173から入力したキーファイルKF1を図32に示す記録モジュール271を介してROM型の記録媒体130のRAM領域132あるいはメディアSAM133内に書き込む。

これにより、購入形態が決定されたROM型の記録媒体130が得られる。

このとき、課金処理部187が生成した利用制御状態データ166および利用 履歴データ108は、所定のタイミングで、スタックメモリ200および外部メモリ201からそれぞれ読み出しされたEMDサービスセンタ102に送信される。

以下、図36に示すように、AV機器160sにおいて購入形態が未決定のROM型の記録媒体130からセキュアコンテナ104を読み出してAV機器160cに転送し、AV機器160cにおいて購入形態を決定してRAM型の記録媒体250に書き込む際の処理の流れを図37および図38を用いて説明する。

図37は、SAM105%における当該処理のフローチャートである。

図38は、SAM1052 における当該処理のフローチャートである。 なお、ROM型の記録媒体 130からRAM型の記録媒体 250へのセキュアコンテナ104の転送は、図1に示すネットワーク機器 1601 およびAV機器 1601 ~1604 のいずれの間で行ってもよい。

ステップSM11 (図37): AV機器160sのSAM105sとROM型の記録媒体130のメディアSAM133との間で相互認証を行い、ROM型の記録媒体130のメディア鍵データKmbdiをSAM105sに転送する。

このとき、同様に、V機器1602のSAM1052とRAM型の記録媒体2

5 0 のメディアSAM 2 5 2 との間で相互認証を行い、RAM型の記録媒体 2 5 0 のメディア鍵データ K M B D 2 を SAM 1 0 5 2 に転送する。

ステップSM12:SAM105sは、RAM領域132から読み出した図4B, CキーファイルKF、署名データSIG7.cp、公開鍵証明書データCERcp およびその署名データSIG1.BSc とを、図40に示す暗号化・復号部172において、対応する期間の配信用鍵データKD1  $\sim$ KDs を用いて順に復号する。

次に、暗号化・復号部172で復号されたコンテンツファイルCFは、暗号化・復号部171に出力され、SAM105。と105。との間の相互認証によって得られたセッション鍵データKses を用いて暗号化された後に、SAM管理部190に出力される。

また、暗号化・復号部172で復号されたキーファイルKFは、暗号化・復号部171および署名処理部189に出力される。

ステップSM13:署名処理部189は、SAM105sの秘密鍵データKsAms.sを用いて、キーファイルKFの署名データSIGs50, SAMSを作成し、これを暗号化・復号部171に出力する。

ステップSM14: 暗号化・復号部171は、記憶部192から読み出したSAM105sの公開鍵証明書データCERsamsおよびその署名データSIGs51.

BSCと、キーファイルKFおよびその署名データSIGs50. SAMSと、ROM型の記録媒体130のROM領域131から読み出した図4Aに示すコンテンツファイルCFとを、SAM105sと1052との間の相互認証によって得られたセッション鍵データKsBsを用いて暗号化した後に、SAM管理部190を介して、AV機器1602のSAM1052に出力する。

ステップSN1 (図38):SAM105 $_2$  では、図41に示すように、SAM管理部190を介してSAM105 $_8$  から入力されたコンテンツファイルCFが、暗号化・復号部171においてセッション鍵データ $_8$  を用いて復号され

た後に、メディアSAM管理部197を介してRAM型の記録媒体250のRA M領域251に書き込まれる。

また、SAM管理部 180を介してSAM105。から入力されたキーファイル KF およびその署名データ  $SIG_{850, SAM8}$ と、公開鍵証明書データ  $CER_{SAM8}$  およびその署名データ  $SIG_{851, BSC}$  とが、スタックメモリ 200 に書き込まれた後に、暗号化・復号部 171 においてセッション鍵データ  $K_{SBS}$  を用いて復号される。

ステップSN2:当該復号された署名データSIG $_{851,BCS}$ が、署名処理部189において署名検証され、その正当性が確認されると、公開鍵証明書データCER $_{8AM3}$ に格納された公開鍵データK $_{8AM3}$ を用いて、署名データSIG $_{850,SAM3}$ の正当性、すなわちキーファイルKFの送信元の正当性が確認される。

そして、署名データSIG $_{350, SAM3}$ の正当性が確認されると、スタックメモリ 200からキーファイルKFが読み出されてセキュアコンテナ復号部 183に出力される。

ステップSN3:セキュアコンテナ復号部183は、対応する期間の配信用鍵 データKD1~KDsを用いて、キーファイルKFを復号し、所定の署名検証を 経た後に、当該復号したキーファイルKFをスタックメモリ200に書き込む。

その後、スタックメモリ200に記憶されている既に復号されたキーファイル KFに格納された権利書データ106が、利用監視部186に出力される。そして、利用監視部186によって、権利書データ106に基づいて、コンテンツの 購入形態および利用形態が管理される。

ステップSN4:課金処理部187において、ユーザによる図16に示す購入
・利用形態決定操作部165の操作によって、試聴モードを示す操作信号S165が発生したか否かが判断され、発生したと判断された場合にはステップSN5の処理が行われ、そうでない場合にはステップSN6の処理が行われる。

ステップSN5:ユーザによって試聴モードが選択されると、既にセッション

鍵データKsBs で復号されたコンテンツファイルCFのコンテンツデータCと、スタックメモリ200に記憶されたコンテンツ鍵データKc、権利書データ106から得られた半開示パラメータデータ199およびユーザ電子透かし情報用データ196とが、相互認証を経た後に、図36に示す復号・伸長モジュール管理部184を介して再生モジュール270に出力される。そして、再生モジュール270において、試聴モードに対応したコンテンツデータCの再生が行われる。

ステップSN6:ユーザによる図36に示す購入・利用形態決定操作部165 の操作によってコンテンツの購入・利用形態が決定され、当該決定に応じた操作 信号S165が、課金処理部187に出力される。

ステップSN7:課金処理部187において、決定された購入・利用形態に応じて利用制御状態データ166および利用履歴データ108が生成され、これがスタックメモリ200および外部メモリ201にそれぞれ書き込まれる。

ステップSN8:スタックメモリ200から読み出された利用制御状態データ 166を格納した例えば図29Bに示すキーファイルKF1が作成され、これが 暗号化・復号部173に出力される。

ステップSN9:暗号化・復号部173において記憶部192から読み出した 記録用鍵データKstr 、メディア鍵データKmedzおよび購入者鍵データKrin を 用いて順に暗号化され、メディアSAM管理部197に出力される。

ステップSN10:メディアSAM管理部197によって、キーファイルKF 1が、図36に示す記録モジュール271によってRAM型の記録媒体250の RAM領域251あるいはメディアSAM252に書き込まれる。

また、利用制御状態データ166および利用履歴データ108は、所定のタイミングで、EMDサービスセンタ102に送信される。

以下、SAM1051~1051の実現方法について説明する。

 $SAM1051 \sim 1051$ の機能をハードウェアとして実現する場合は、メモリを内蔵したASIC型のCPUを用いて、そのメモリには、図17に示す各機

能を実現するためのセキュリティー機能モジュールやコンテンツの権利処理をおこなうプログラムモジュールおよび鍵データなどの機密度の高いデータが格納される。暗号ライブラリーモジュール(公開鍵暗号、共通鍵暗号、乱数発生器、ハッシュ関数)、コンテンツの使用制御用のプログラムモジュール、課金処理のプログラムモジュールなど、一連の権利処理用のプログラムモジュールは、例えば、ソフトウェアとして実装される。

例えば、図17に示す暗号化・復号部171などのモジュールは、例えば、処理速度の問題でハードウエアとしてASIC型のCPU内のIPコアとして実装される。クロック速度やCPUコード体系などの性能によっては、暗号化・復号部171をソフトウェアとして実装してもよい。

また、図17に示す記憶部182や、図17に示す機能を実現するためのプログラムモジュールおよびデータを格納するメモリとしては、例えば、不揮発メモリー(フラッシューROM)が用いられ、作業用メモリとしてはSRAMなどの高速書き込み可能なメモリが用いられる。なお、その他にも、SAM1051~105。に内蔵されるメモリとして、強誘電体メモリー(FeRAM)を用いてもよい。

また、SAM1051~1051には、その他に、コンテンツの利用のための有効期限や契約期間などで日時の検証に使用する時計機能が内蔵されている。

上述したように、SAM1051~1051は、プログラムモジュールや、データおよび処理内容を外部から遮蔽した耐タンパ性の構造を持っている。SAM1051~1051を搭載した機器のホストCPUのバス経由で、当該SAMのIC内部のメモリに格納されている秘密性の高いプログラムおよびデータの内容や、SAMのシステムコンフィギュレーション(System Configuration)関連のレジスタ群および暗号ライブラリーや時計のレジスタ群などの値が、読み出されたり、新規に書き込まれたりしないように、すなわち、搭載機器のホストCPUが割り付けているアドレス空間内に存在しないように、当該SAMでは、CPU側

のメモリー空間を管理するMMU(Memory Magagement Unit)を用いて、搭載機器 側のホストCPUからは見えないアドレス空間を設定する。

また、SAM1051~~1051は、X線や熱などの外部からの物理的な攻撃にも耐え得る構造をもち、さらにデバッグ用ツール(ハードウエアICE、ソフトウエアICE)などを用いたリアルタイムデバッグ(リバースエンジニアリング)が行われても、その処理内容が分からないか、あるいは、デバッグ用ツールそのものがIC製造後には使用できないような構造をしている。

 $SAM1051\sim1054$  自身は、ハードウエア的な構造においては、メモリを内蔵した通常のASIC型のCPUであり、機能は当該CPUを動作させるソフトウェアに依存するが、暗号機能と耐タンパ性のハードウェア構造を有している点が、一般的なASIC型のCPUと異なる。

SAM1051~1051の機能を全てソフトウエアで実現する場合は、耐タンパ性を持ったモジュール内部で閉じてソフトウエア処理をおこなう場合と、通常のセットに搭載されているホストCPU上のソフトウエア処理で行い、当該処理のときにのみ解読することが不可能となる仕掛けをする場合とがある。前者は、暗号ライブラリモジュールがIPコアではなく、通常のソフトウェアモジュールとしてメモリに格納される場合と同じであり、ハードウェアとして実現する場合と同様に考えられる。一方、後者は、タンパーレジスタントソフトウェアと呼ばれるもので、ICE(デバッガ)で実行状況を解読されても、そのタスクの実行順序がバラバラであったり(この場合には、区切ったタスク単体でプログラムとしての意味があるように、すなわち前後のラインに影響がでないようにタスク切りを行う)、タスクそのものが暗号化されており、一種のセキュア処理を目的としたタスクスケジューラ(MiniOS)と同様に実現できる。当該タスクスケジューラは、ターゲットプログラムに埋め込まれている。

次に、図16に示す復号・伸長モジュール163について説明する。

図16に示すように、復号・伸長モジュール163は、相互認証部220、復

号部221、復号部222、伸長部223、電子透かし情報処理部224および 半開示処理部225を有する。

相互認証部220は、復号・伸長モジュール163がSAM1051からデータを入力する際に、図26に示す相互認証部170との間で相互認証を行ってセッション鍵データKsss を生成する。

復号部221は、SAM1051から入力したコンテンツ鍵データKc、半開示パラメータデータ199、ユーザ電子透かし情報用データ196およびコンテンツデータCを、セッション鍵データKsBs を用いて復号する。そして、復号部221は、復号したコンテンツ鍵データKcおよびコンテンツデータCを復号部221は、復号したユーザ電子透かし情報用データ196を電子透かし情報処理部224に出力し、半開示パラメータデータ199を半開示処理部225に出力する。

復号部222は、半開示処理部225からの制御に基づいて、コンテンツ鍵データKcを用いて、コンテンツデータCを半開示状態で復号し、復号したコンテンツデータCを伸長部223に出力する。

伸長部223は、復号されたコンテンツデータCを伸長して、電子透かし情報 処理部224に出力する。

伸長部223は、例えば、図4Aに示すコンテンツファイルCFに格納された A/V伸長用ソフトウェアを用いて伸長処理を行い、例えば、ATRAC3方式 で伸長処理を行う。

電子透かし情報処理部224は、復号されたユーザ電子透かし情報用データ196に応じたユーザ電子透かし情報を、復号されたコンテンツデータCに埋め込み、新たなコンテンツデータCを生成する。電子透かし情報処理部224は、当該新たなコンテンツデータCを再生モジュール169に出力する。

このように、ユーザ電子透かし情報は、コンテンツデータCを再生するときに、 復号・伸長モジュール163において埋め込まれる。

なお、本発明では、コンテンツデータCにユーザ電子透かし情報用データ196を埋め込まないようにしてもよい。

半開示処理部225は、半開示パラメータデータ189に基づいて、例えば、 コンテンツデータCのうち復号を行わないブロックと、復号を行うブロックとを 復号部222に指示する。

また、半開示処理部225は、その他に、半開示パラメータデータ199に基づいて、試聴時の再生機能を限定したり、試聴可能な期間を限定するなどの制御を行う。

再生モジュール 1 6 8 は、復号および伸長されたコンテンツデータ C に応じた 再生を行う。

次に、コンテンツプロバイダ101、EMDサービスセンタ102およびユーザホームネットワーク103の間で、秘密鍵データを用いて生成した署名データを付したデータおよび公開鍵証明書データを送受信する際のデータフォーマットについて説明する。

図42Aは、コンテンツプロバイダ101からSAM1051にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ101からSAM1051に、コンテンツプロバイダ101とSAM1051との間の相互認証によって得たセッション鍵データ $K_{SBS}$ で暗号化したモジュールMod50が送信される。

モジュール $M \circ d \circ c$ は、モジュール $M \circ d \circ 1$ およびその秘密鍵データK c p. sによる署名データS I G c pが格納されている。

このように、公開鍵証明書データCER $_{cP}$ を格納したモジュール $_{MO}$  d  $_{50}$ を、コンテンツプロバイダ $_{1}$  0 1 から $_{SAM105}$  に送信することで、 $_{SAM105}$  において署名データ $_{SIGcP}$ の検証を行なう際に、 $_{EMD}$  サービスセンタ  $_{1}$  0 2 から $_{SAM105}$  に公開鍵証明書データ $_{CERcP}$ を送信する必要がなくなる。

図42B、図42Cは、コンテンツプロバイダ101からSAM1051にデータDataをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ101からSAM1051に、コンテンツプロバイダ101とSAM1051との間の相互認証によって得たセッション鍵データ $K_{SBS}$ で暗号化した図42Bに示すモジュール $Mod_{52}$ が送信される。

モジュールMods2には、送信するデータDataと、その秘密鍵データKcp.sによる署名データSIGcpとが格納されている。

また、EMDサービスセンタ102からSAM1051には、EMDサービスセンタ102とSAM1051との間の相互認証によって得たセッション鍵データ $K_{SBS}$ で暗号化した図42Cに示すモジュール $M_{O}$ d $_{58}$ が送信される。

モジュール $M \circ d_{58}$ には、コンテンツプロバイダ $1 \circ 1 \circ 0 \circ 1 \circ 0$  類鍵証明書データ  $C \in R_{CP}$  と、その秘密鍵データ $K_{BSC}$  。 による署名データ $S \mid G_{BSC}$  とが格納されている。

図42Dは、SAM1051からコンテンツプロバイダ101にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、SAM1051 からコンテンツプロバイダ101に、コンテンツプロバイダ101とSAM1051 との間の相互認証によって得たセッション鍵データ $K_{SBS}$  で暗号化したモジュールMods4が送信される。

モジュールMods₄には、モジュールModsҕおよびその秘密鍵データKѕѧмュ

,sによる署名データSIGsamiが格納されている。

モジュールMods5には、SAM1051の秘密鍵データKsam1, pを格納した公開鍵証明書データCERsam1と、公開鍵証明書データCERsam1に対しての秘密鍵データKesc, s による署名データSIGesc と、送信するデータDataとが格納されている。

このように、公開鍵証明書データCERsamiを格納したモジュールModssを、SAM1051からコンテンツプロバイダ101に送信することで、コンテンツプロバイダ101において署名データSIGsamiの検証を行なう際に、EMDサービスセンタ102からコンテンツプロバイダ101に公開鍵証明書データCERsamiを送信する必要がなくなる。

図42E、図42Fは、SAM1051からコンテンツプロバイダ101にデータDataをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、SAM1051 からコンテンツプロバイダ101に、コンテンツプロバイダ101とSAM1051 との間の相互認証によって得たセッション鍵データ $K_{SBS}$  で暗号化した図42Eに示すモジュールMod58が送信される。

モジュールModsmには、送信するデータDataと、その秘密鍵データKsami.sによる署名データSIGsamiとが格納されている。

また、EMDサービスセンタ102からコンテンツプロバイダ101には、EMDサービスセンタ102とコンテンツプロバイダ101との間の相互認証によって得たセッション鍵データ $K_{SBS}$ で暗号化した図42Fに示すモジュール $Mod_{57}$ が送信される。

モジュールMods7には、SAM1051の公開鍵証明書データCERsAM1と、その秘密鍵データKBSC, Sによる署名データSIGBSCとが格納されている。

図43Aは、コンテンツプロバイダ101からEMDサービスセンタ102に データDataをイン・バンド方式で送信する場合のデータフォーマットを説明

するための図である。

この場合には、コンテンツプロバイダ101からEMDサービスセンタ102に、コンテンツプロバイダ101とEMDサービスセンタ102との間の相互認証によって得たセッション鍵データ $K_{SBS}$ で暗号化したモジュール $Mod_{58}$ が送信される。

モジュールModssには、モジュールModssおよびその秘密鍵データKcp.s による署名データSIGcpが格納されている。

図43Bは、コンテンツプロバイダ101からEMDサービスセンタ102に データDataをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ101からEMDサービスセンタ102に、コンテンツプロバイダ101とEMDサービスセンタ102との間の相互認証によって得たセッション鍵データ $K_{SBS}$ で暗号化した図43Bに示すモジュール $M_0d_{80}$ が送信される。

モジュールModeoには、送信するデータDataと、その秘密鍵データKcp.sによる署名データSIGcpとが格納されている。

このとき、EMDサービスセンタ102にはコンテンツプロバイダ101の公 開鍵証明書データCERcpは既に登録されている。

図43Cは、SAM1051からEMDサービスセンタ102にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、SAM1051からEMDサービスセンタ102に、EMDサ

ービスセンタ102とSAM1051との間の相互認証によって得たセッション 鍵データKsbs で暗号化したモジュールMode1が送信される。

モジュールMode1には、モジュールMode2およびその秘密鍵データKsam1.sによる署名データSIGsam1が格納されている。

モジュール $M \circ d_{82}$ には、SAM1051 の秘密鍵データ $K_{SAM1.P}$ を格納した公開鍵証明書データ $CER_{SAM1}$ と、公開鍵証明書データ $CER_{SAM1}$ に対しての秘密鍵データ $K_{BSC.S}$  による署名データ $SIG_{BSC}$  と、送信するデータDataとが格納されている。

図43Dは、SAM1051からEMDサービスセンタ102にデータDataをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、SAM1051からEMDサービスセンタ102に、EMDサービスセンタ102とSAM1051との間の相互認証によって得たセッション鍵データ $K_{SBS}$ で暗号化した図43Dに示すモジュール $Mod_{85}$ が送信される。

モジュールModesには、送信するデータDataと、その秘密鍵データKsami.sによる署名データSIGsamiとが格納されている。

このとき、EMDサービスセンタ102にはSAM1051の公開鍵証明書データCERsam1は既に登録されている。

以下、 $SAM1051 \sim 105$  の出荷時におけるEMDサービスセンタ10 2への登録処理について説明する。

なお、 $SAM1051\sim105$ 。の登録処理は同じであるため、以下、SAM1051の登録処理について述べる。

SAM1051の出荷時には、図11に示すEMDサービスセンタ102の鍵サーバ141によって、SAM管理部149を介して、図17などに示す記憶部192に以下に示す鍵データが初期登録される。

また、SAM1051には、例えば、出荷時に、記憶部192などに、SAM

105.がEMDサービスセンタ102に初回にアクセスする際に用いられるプログラムなどが記憶される。

すなわち、記憶部 192には、例えば、図 21において左側に「\*」が付されている SAM1051の識別子  $SAM\_ID$ 、記録用鍵データ $K_{STR}$ 、ルート認証局 2の公開鍵データ $K_{R-CA}$ 、EMDサービスセンタ 102の公開鍵データ $K_{BS}$  C.P、SAM1051 の秘密鍵データ $K_{SAM1}$ . S、公開鍵証明書データ  $CER_{SAM1}$  およびその署名データ  $SIG_{22.BSC}$ 、復号・伸長モジュール 163 およびメディア SAM との間の認証用鍵データを生成するための元鍵データが初期登録で記憶される。

なお、公開鍵証明書データCER<sub>SAM1</sub>は、SAM1051を出荷後に登録する際にEMDサービスセンタ102からSAM1051に送信してもよい。

ここで、ルート認証局 2 の公開鍵データ $K_{R-CA}$ は、インターネットの電子商取引などでは一般的に使用されているRSAを使用し、データ長は例えば 1 0 2 4 ビットである。公開鍵データ $K_{R-CA}$ は、図1 に示すルート認証局 2 によって発行される。

また、EMDサービスセンタ102の公開鍵データKBSC、Pは、短いデータ長でRSAと同等あるいはそれ以上の強度を持つ楕円曲線暗号を利用して生成され、データ長は例えば160ビットである。但し、暗号化の強度を考慮すると、公開鍵データKBSC、Pは192ビット以上であることが望ましい。また、EMDサービスセンタ102は、ルート認証局92に公開鍵データKBSC、Pを登録する。

また、ルート認証局 92 は、公開鍵データ $K_{BSC,P}$  の公開鍵証明書データCE  $R_{BSC}$  を作成する。公開鍵データ $K_{BSC,P}$  を格納した公開鍵証明書データCER BSC は、好ましく、SAM1051 の出荷時に記憶部 192 に記憶される。この場合に、公開鍵証明書データ $CER_{BSC}$  は、ルート認証局 92 の秘密鍵データ $K_{ROOT,S}$ で署名されている。

EMDサービスセンタ102は、乱数を発生してSAM1051の秘密鍵デー

タ K sam1. s、を生成し、これとペアとなる公開鍵データ K sam1. pを生成する。 また、E M D サービスセンタ 1 0 2 は、ルート認証局 9 2 の認証をもらって、

公開鍵データK<sub>SAM1, P</sub>の公開鍵証明書データCER<sub>SAM1</sub>を発行し、これに自らの 秘密鍵データK<sub>BSC, S</sub>を用いて署名データを添付する。すなわち、EMDサービ スセンタ102は、セカンドCA(認証局)として機能を果たす。

また、SAM1051には、図11に示すEMDサービスセンタ102のSAM管理部149により、EMDサービスセンタ102の管理下にある一意(ユニーク)な識別子SAM\_IDが割り当てられ、これがSAM1051の記憶部192に格納されると共に、図11に示すSAMデータベース149aにも格納され、EMDサービスセンタ102によって管理される。

また、SAM1051は、出荷後、例えば、ユーザによってEMDサービスセンタ102と接続され、登録手続を行うと共に、EMDサービスセンタ102から記憶部192に配信用鍵データKD1~KD8が転送される。

すなわち、SAM1051 を利用するユーザは、コンテンツをダウンロードする前にEMDサービスセンタ102 に登録手続が必要である。この登録手続は、例えば、SAM1051 を搭載している機器(当該例では、ネットワーク機器1601)を購入したときに添付された登録用紙などを用いて、ユーザ本人が自己を特定する情報を記載して例えば郵便などのオフラインで行なわれる。

SAM1051は、上述した登録手続を経た後でないと使用できない。

EMDサービスセンタ102は、SAM1051のユーザによる登録手続に応じて、ユーザに固有の識別子USER\_IDを発行し、例えば、図11に示すSAMデータベース149aにおいて、SAM\_IDとUSER\_IDとの対応関係を管理し、課金時に利用する。

また、EMDサービスセンタ102は、SAM1051のユーザに対して情報 参照用識別子IDと、初回に使用されるパスワードを割り当て、これをユーザに 通知する。ユーザは、情報参照用識別子IDとパスワードとを用いて、EMDサ

ービスセンタ102に、例えば現在までのコンテンツデータの利用状況(利用履歴)などを情報の問い合わせを行なうことができる。

また、EMDサービスセンタ102は、ユーザの登録時に、クレジットカード 会社などに身分の確認を行なったり、オフラインで本人の確認を行なう。

次に、図21に示すように、SAM1051内の記憶部192にSAM登録リストを格納する手順について説明する。

図1に示すSAM1051は、例えば、バス191としてIEEE1394シリアルバスを用いた場合に、バス191に接続された機器の電源を立ち上げたり、新しい機器をバス191に接続したときに生成されるトポロジーマップを利用して、自分の系に存在するSAM1052~SAM1051のSAM2録リストを得る。

なお、IEEE1394シリアルバスであるバス191に応じて生成されたトポロジーマップは、例えば、図44に示すように、バス191にSAM1051 $\sim$ 105。に加えてAV機器160 $_{5}$ , 160。のSCMS処理回路105 $_{5}$ , 105。が接続されている場合に、SAM105 $_{1}$   $\sim$ 105、およびSCMS処理回路105 $_{5}$ , 105。を対象として生成される。

従って、SAM1051 は、当該トポロジーマップから、SAM1051 ~ 1 0 5 4 についての情報を抽出してSAM登録リストを生成する。

SAM登録リストのデータフォーマットは、例えば、図45に示される。 そして、SAM1051は、当該SAM登録リストを、EMDサービスセンタ 102に登録して署名を得る。

これらの処理は、バス191のセッションを利用してSAM105」が自動的に行い、EMDサービスセンタ102にSAM登録リストの登録命令を発行する

EMDサービスセンタ102は、SAM1051から図45に示すSAM登録リストを受けると、有効期限を確認する。そして、EMDサービスセンタ102

は、登録時にSAM1051より指定された決済機能の有無を参照して対応する 部分の設定を行う。また、EMDサービスセンタ102は、リボケーションリス トをチェックしてSAM登録リスト内のリボケーションフラグを設定する。リボ ケーションリストは、例えば、不正使用などを理由にEMDサービスセンタ10 2によって使用が禁止されている(無効な)SAMのリストである。

また、EMDサービスセンタ102は、決済時にはSAM1051に対応する SAM登録リストを取り出し、その中に記述されたSAMがリボケーションリス トに含まれているかを確認する。また、EMDサービスセンタ102は、SAM 登録リストに署名を添付する。

なお、SAMリホケーションリストは、同一系の(同一のバス191に接続されている)SAMのみを対象として生成され、各SAMに対応するリボケーションンフラグによって、当該SAMの有効および無効を示している。

以下、図1に示すコンテンツプロバイダ101の全体動作について説明する。 図46は、コンテンツプロバイダ101の全体動作のフローチャートである。

ステップS1:EMDサービスセンタ102は、コンテンツプロバイダ101 が所定の登録処理を経た後に、コンテンツプロバイダ101の公開鍵データKcp pの公開鍵証明書CERcpをコンテンツプロバイダ101に送信する。

また、EMDサービスセンタ102は、SAM1051~1054が所定の登録処理を経た後に、SAM1051~1054の公開鍵データК sam1, p~К sam4.pの公開鍵証明書CERcp1~CERcp4をSAM1051~1054に送信する。

また、EMDサービスセンタ102は、相互認証を行った後に、各々有効期限が1カ月の6カ月分の配信用鍵データKD<sub>1</sub>  $\sim$  KD<sub>8</sub> をコンテンツプロバイダ101に送信し、3カ月分の配信用鍵データKD<sub>1</sub>  $\sim$  KD<sub>8</sub> をユーザホームネットワーク103に送信する。

このように、EMDシステム100では、配信用鍵データKD1~KDsを予

めSAM105、 $\sim$ 105、に配給しているため、SAM105、 $\sim$ 105、とEMDサービスセンタ102との間がオフラインの状態でも、SAM105、 $\sim$ 105、においてコンテンツプロバイダ101から配給されたセキュアコンテナ104を復号して購入・利用できる。この場合に、当該購入・利用の履歴は利用履歴データ108に記述され、利用履歴データ108は、SAM105、 $\sim$ 105、とEMDサービスセンタ102とが接続されたときに、EMDサービスセンタ102に自動的に送信されるため、EMDサービスセンタ102における決済処理を確実に行うことができる。なお、EMDサービスセンタ102が、所定の期間内に、利用履歴データ108を回収できないSAMについては、リボケーションリストで無効の対象とする。

なお、利用制御状態データ 166 は、原則として、リアルタイムで、 $SAM105_1 \sim 105_4$  からEMDサービスセンタ 102 に送信される。

ステップS 2: コンテンツプロバイダ 1 0 1 は、相互認証を行った後に、図 7 A に示す権利登録要求モジュールM o d 2 を、E M D サービスセンタ 1 0 2 に送信する。

そして、EMDサービスセンタ102は、所定の署名検証を行った後に、権利 書データ106およびコンテンツ鍵データKcを登録して権威化する。

ステップS3:コンテンツプロバイダ101は、対応する期間の配信用鍵データKD1~KD。などを用いて暗号化を行って、図4A,Bに示すコンテンツファイルCFおよびキーファイルKFを作成し、これらと図4Cに示す公開鍵証明書データCERェとを格納したセキュアコンテナ104を、オンラインおよび/またはオフラインで、ユーザホームネットワーク103に配給する。

テンツプロバイダ101から送信されたか否かを確認する。

ステップS 5: SAM 1 0 5 1 ~SAM 1 0 5 4 において、ユーザによる図 1 6 に示す購入・利用形態決定操作部 1 6 5 の操作に応じた操作信号S 1 6 5 に基づいて、購入・利用形態を決定する。

このとき、図23に示す利用監視部186において、セキュアコンテナ104 に格納された権利書データ106に基づいて、ユーザによるコンテンツファイル CFの購入・利用形態が管理される。

ステップS 6: S A M 1 O 5:  $\sim$  S A M 1 O 5: の図 2 3 に示す課金処理部 1 8 7 において、操作信号S 1 6 5 に基づいて、ユーザによる購入・利用形態の決定の操作を記述した利用履歴データ 1 O 8 および利用制御状態データ 1 G 6 が生成し、これらを E M D サービスセンタ 1 O 2 に送信する。

ステップS7:EMDサービスセンタ102は、図11に示す決算処理部142において、利用履歴データ108に基づいて決済処理を行い、決済請求権データ152および決済レポートデータ107を作成する。EMDサービスセンタ102は、決済請求権データ152およびその署名データSIG88を、図1に示すペイメントゲートウェイ90を介して、決済機関91に送信する。また、EMDサービスセンタ102は、決済レポートデータ107をコンテンツプロバイダ101に送信する。

ステップS8:決済機関91において、署名データSIG88の検証を行った後に、決済請求権データ152に基づいて、ユーザが支払った金額が、コンテンツプロバイダ101の所有者に分配される。

以上説明したように、EMDシステム100では、図4に示すフォーマットのセキュアコンテナ104をコンテンツプロバイダ101からユーザホームネットワーク103に配給し、セキュアコンテナ104内のキーファイルKFについての処理をSAM1051~105。内で行う。

また、キーファイルKFに格納されたコンテンツ鍵データKcおよび権利書デ

ータ106は、配信鍵データ $KD_1 \sim KD_8$  を用いて暗号化されており、配信鍵データ $KD_1 \sim KD_8$  を保持している $SAM105_1 \sim 105_4$  内でのみ復号される。そして、 $SAM105_1 \sim 105_4$  では、耐タンパ性を有するモジュールであり、権利書データ106に記述されたコンテンツデータCの取り扱い内容に基づいて、コンテンツデータCの購入形態および利用形態が決定される。

従って、EMDシステム100によれば、ユーザホームネットワーク103におけるコンテンツデータCの購入および利用を、コンテンツプロバイダ101の関係者が作成した権利書データ106の内容に基づいて確実に行わせることができる。

また、EMDシステム100では、コンテンツプロバイダ101からユーザホームネットワーク103へのコンテンツデータCの配給を、オンラインおよびオフラインの何れの場合でもセキュアコンテナ104を用いて行うことで、SAM1051~1054におけるコンテンツデータCの権利処理を双方の場合において共通化できる。

また、EMDシステム100では、ユーザホームネットワーク103内のネットワーク機器1601 およびAV機器1602 ~1604 においてコンテンツデータCを購入、利用、記録および転送する際に、常に権利書データ106に基づいて処理を行うことで、共通の権利処理ルールを採用できる。

## 第1実施形態の第1変形例

上述した実施形態では、図4Bに示すように、コンテンツプロバイダ101において配信用鍵データKDを用いてキーファイルKFを暗号化し、SAM105 $_1\sim105$ 。において配信用鍵データKDを用いてキーファイルKFを復号する場合を例示したが、図1に示すように、コンテンツプロバイダ101からSAM105 $_1\sim105$ 。にセキュアコンテナ104を直接供給する場合には、配信用鍵データKDを用いたキーファイルKFの暗号化は必ずしも行なわなくてもよい

このように、配信用鍵データKDを用いてキーファイルKFを暗号化することは、後述する第2実施形態のように、コンテンツプロバイダからユーザホームネットワークにサービスプロバイダを介してコンテンツデータを供給する場合に、配信用鍵データKDをコンテンツプロバイダおよびユーザホームネットワークにのみ保持させることで、サービスプロバイダによる不正行為を抑制する際に大きな効果を発揮する。

但し、上述した第1実施形態の場合でも、配信用鍵データKDを用いてキーファイルKFを暗号化することは、コンテンツデータの不正利用の抑制力を高める点で効果がある。

また、上述した実施形態では、図4Bに示すキーファイルKF内の権利書データ106内に標準小売価格データSRPを格納する場合を例示したが、セキュアコンテナ104内のキーファイルKFの外に、標準小売価格データSRP(プライスタグデータ)を格納してもよい。この場合には、標準小売価格データSRPに対して秘密鍵データKcpを用いて作成した署名データを添付する。

## 第1実施形態の第2変形例

上述した第1実施形態では、図1に示すように、EMDサービスセンタ102が、自らが生成した決済請求権データ152を用いて、ペイメントゲートウェイ90を介して決済機関91で決済処理を行なう場合を例示したが、例えば、図47に示すように、EMDサービスセンタ102からコンテンツプロバイダ101に決済請求権データ152を送信し、コンテンツプロバイダ101自らが、決済請求権データ152を用いて、ペイメントゲートウェイ90を介して決済機関91に対して決済処理を行なってもよい。

## 第1実施形態の第3変形例

上述した第1実施形態では、単数のコンテンツプロバイダ101からユーザホームネットワーク103のSAM1051~105.に、セキュアコンテナ104を供給する場合を例示したが、2以上のコンテンツプロバイダ101a,10

1 bからSAM1051~1054にそれぞれセキュアコンテナ104a, 104bを供給するようにしてもよい。

図48は、コンテンツプロバイダ101a, 101bを用いる場合の第1実施 形態の第3変形例に係わるEMDシステムの構成図である。

この場合には、EMDサービスセンタ102は、コンテンツプロバイダ101 a および101 b に、それぞれ6 カ月分の配信用鍵データKD a 1 ~KD b 2 を配信する。

また、EMDサービスセンタ102は、SAM1051~105. に、3カ月 分の配信用鍵データKDa1~KDasおよびKDb1~KDbsを配信する。

そして、コンテンツプロバイダ101aは、独自のコンテンツ鍵データKca を用いて暗号化したコンテンツファイルCFaと、コンテンツ鍵データKca および権利書データ106aなどを対応する期間の配信用鍵データKDaι  $\sim$  K D a。を用いて暗号化したキーファイルKFaとを格納したセキュアコンテナ10 4 a を S A M 1 0 5  $\iota$  ~ 1 0 5  $\iota$  にオンラインおよび/またはオフランで供給する。

このとき、キーファイルの識別子として、EMDサービスセンタ102が配付するグローバルユニークな識別子Content\_IDが用いられ、EMDサービスセンタ102によって、コンテンツデータが一元的に管理される。

また、コンテンツプロバイダ101bは、独自のコンテンツ鍵データKcbを用いて暗号化したコンテンツファイルCFbと、コンテンツ鍵データKcbおよび権利書データ106bなどを対応する期間の配信用鍵データKDb1~KDb6。を用いて暗号化したキーファイルKFb6とを格納したセキュアコンテナ104b6をSAM1051~1051。にオンラインおよび/またはオフランで供給する

SAM1051~105。は、セキュアコンテナ104aについては、対応する期間の配信用鍵データKDa1~KDa8を用いて復号を行い、所定の署名検

証処理などを経てコンテンツの購入形態を決定し、当該決定された購入形態および利用形態などに応じて生成した利用履歴データ108 a および利用制御状態データ166 a をEMDサービスセンタ102 に送信する。

また、SAM1051~~1054は、セキュアコンテナ104bについては、 対応する期間の配信用鍵データKDb1~~KDb8を用いて復号を行い、所定の 署名検証処理などを経てコンテンツの購入形態を決定し、当該決定された購入形態および利用形態などに応じて生成した利用履歴データ108bおよび利用制御 状態データ166bをEMDサービスセンタ102に送信する。

EMDサービスセンタ102では、利用履歴データ108aに基づいて、コンテンツプロバイダ101aについての決済請求権データ152aを作成し、これを用いて決済機関91に対して決済処理を行なう。

また、EMDサービスセンタ102では、利用履歴データ108bに基づいて、コンテンツプロバイダ101bについての決済請求権データ152bを作成し、これを用いて決済機関91に対して決済処理を行なう。

また、EMDサービスセンタ102は、権利書データ106a, 106bを登録して権威化を行なう。このとき、EMDサービスセンタ102は、権利書データ106a, 106bに対応するキーファイルKFa, KFbに対して、グローバルユニークな識別子Content\_IDを配付する。

また、EMDサービスセンタ102は、コンテンツプロバイダ101a, 101bの公開鍵証明書データCER $c_Pa$ , CER $c_Pb$  を発行し、これに自らの署名データSIG<sub>1b</sub>, BSC, SIG<sub>1a</sub>, BSCを付してその正当性を認証する。

## 第2実施形態

上述した実施形態では、コンテンツプロバイダ101からユーザホームネットワーク103のSAM1051~1054にコンテンツデータを直接配給する場合を例示したが、本実施形態では、コンテンツプロバイダが提供するコンテンツデータを、サービスプロバイダを介してユーザホームネットワークのSAMに配

給する場合について説明する。

図49は、本実施形態のEMDシステム300の構成図である。

図49に示すように、EMDシステム300は、コンテンツプロバイダ301 、EMDサービスセンタ302、ユーザホームネットワーク303、サービスプロバイダ310、ペイメントゲートウェイ90および決済機関91を有する。

コンテンツプロバイダ301、EMDサービスセンタ302、SAM3051 ~305。およびサービスプロバイダ310は、それぞれ本発明のデータ提供装 置、管理装置、データ処理装置およびデータ配給装置に対応している。

コンテンツプロバイダ301は、サービスプロバイダ310に対してコンテンツデータを供給する点を除いて、前述した第1実施形態のコンテンツプロバイダ101と同じである。

また、EMDサービスセンタ302は、コンテンツプロバイダ101およびS  $AM505_1 \sim 505_1$  に加えて、サービスプロバイダ310に対しても認証機能、鍵データ管理機能および権利処理機能を有する点を除いて、前述した第1実施形態のEMDサービスセンタ102と同じである。

また、ユーザホームネットワーク303は、ネットワーク機器3601 および AV機器3602 ~3604 を有している。ネットワーク機器3601 はSAM 3051 およびCAモジュール311を内蔵しており、AV機器3602 ~3604 はそれぞれSAM3052 ~3054 を内蔵している。

ここで、SAM3051~~3050は、サービスプロバイダ310からセキュアコンテナ304の配給を受ける点と、コンテンツプロバイダ301に加えてサービスプロバイダ310についての署名データの検証処理およびSP用購入履歴データ(データ配給装置用購入履歴データ)309の作成を行なう点とを除いて、前述した第1実施形態のSAM1051~~1050と同じである。

先ず、EMDシステム300の概要について説明する。

EMDシステム300では、コンテンツプロバイダ301は、自らが提供しよ

うとするコンテンツのコンテンツデータCの使用許諾条件などの権利内容を示す 前述した第1実施形態と同様の権利書(UCP:Usage Control Policy)データ106 を、高い信頼性のある権威機関であるEMDサービスセンタ302に送信する。 権利書データ106は、EMDサービスセンタ302に登録されて権威化(認証)される。

また、コンテンツプロバイダ301は、コンテンツ鍵データKcでコンテンツデータCを暗号化してコンテンツファイルCFを生成する。また、コンテンツプロバイダ301は、EMDサービスセンタ302から配給された対応する期間の配信用鍵データKD1~KD。を用いて、コンテンツ鍵データKcおよび権利書データ106を暗号化し、それらを格納したキーファイルKFを作成する。そして、コンテンツプロバイダ301は、コンテンツファイルCF、キーファイルKFおよび自らの署名データとを格納したセキュアコンテナ104を、インターネットなどのネットワーク、デジタル放送、記録媒体あるいは非公式なプロトコルを用いて、あるいはオフラインなどでサービスプロバイダ310に供給する。

サービスプロバイダ310は、コンテンツプロバイダ301からセキュアコンテナ104を受け取ると、署名データの検証を行なって、セキュアコンテナ104が正当なコンテンツプロバイダ301によって作成されたものであるか、並びに送り主の正当性を確認する。

次に、サービスプロバイダ310は、例えばオフラインで通知されたコンテンツプロバイダ301が希望するコンテンツに対しての価格(SRP)に、自らのサービスの価格を加算した価格を示すプライスタグデータ(PT)312を作成する。

そして、サービスプロバイダ310は、セキュアコンテナ104から取り出したコンテンツファイルCFおよびキーファイルKFと、プライスタグデータ31 2と、これらに対しての自らの秘密鍵データKsp.sによる署名データとを格納したセキュアコンテナ304を作成する。

このとき、キーファイルKFは、配信用鍵データ $KD_1 \sim KD_8$  によって暗号化されており、サービスプロバイダ310は当該配信用鍵データ $KD_1 \sim KD_8$ を保持していないため、サービスプロバイダ310はキーファイルKFの中身を見たり、書き換えたりすることはできない。

また、EMDサービスセンタ302は、プライスタグデータ312を登録して 権威化する。

サービスプロバイダ310は、オンラインおよび/またはオフラインでセキュアコンテナ304をユーザホームネットワーク303に配給する。

このとき、オフラインの場合には、セキュアコンテナ304はSAM3051  $\sim 305$  にそのまま供給される。一方、オンラインの場合には、サービスプロバイダ310とCAモジュール311との間で相互認証を行い、セキュアコンテナ304をサービスプロバイダ310においてセッション鍵データKsss を用いた暗号化して送信し、CAモジュール311において受信したセキュアコンテナ304をセッション鍵データKsss を用いて復号した後に、SAM3051  $\sim 305$ 4 に転送する。

次に、 $SAM3051 \sim 3051$  において、セキュアコンテナ304を、EM Dサービスセンタ302から配給された対応する期間の配信用鍵データ $KD1 \sim KD1$  を用いて復号した後に、署名データの検証処理を行う。

SAM305 $_1$  ~305 $_4$  に供給されたセキュアコンテナ30 $_4$  は、ネットワーク機器360 $_1$  およびAV機器360 $_2$  ~360 $_4$  において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。

SAM3051~3054は、上述したセキュアコンテナ304の購入・利用の履歴を利用履歴(Usage Log) データ308として記録する。

利用履歴データ(履歴データまたは管理装置用履歴データ)308は、例えば 、EMDサービスセンタ302からの要求に応じて、ユーザホームネットワーク

303からEMDサービスセンタ302に送信される。

EMDサービスセンタ302は、利用履歴データ308に基づいて、コンテンツプロバイダ301およびサービスプロバイダ310の各々について、課金内容を決定(計算)し、その結果に基づいて、ペイメントゲートウェイ90を介して銀行などの決済機関91に決済を行なう。これにより、ユーザホームネットワーク103のユーザが支払った金銭が、EMDサービスセンタ102による決済処理によって、コンテンツプロバイダ101およびサービスプロバイダ310に分配される。

本実施形態では、第1実施形態と同様に、デジタルのコンテンツデータCをカプセル化して提供することで、従来の記録媒体と密着したデジタルコンテンツを、記録媒体から切り離して、デジタルコンテンツ単体に存在価値を持たせることができる。

ここで、セキュアコンテナは、どのような流通経路(配送チャンネル)を介して提供されても、コンテンツデータC(商品)を販売するときの最も基本となる商品カプセルである。具体的には、セキュアコンテナは、課金を行うための暗号情報や、コンテンツデータCの中身の正当性、コンテンツデータを作成した者の正当性およびコンテンツデータの流通業者の正当性を検証するための署名データや、コンテンツデータに埋め込む電子透かし情報に関する情報などの著作権に係わる情報を含む商品カプセルである。

また、本実施形態では、EMDサービスセンタ302は、認証機能、鍵データ管理機能および権利処理(利益分配)機能を有している。

すなわち、EMDサービスセンタ302は、中立の立場にある最高の権威機関であるルート認証局92に対してのセカンド認証局(Second Certificate Author ity)としての役割を果たし、コンテンツプロバイダ301、サービスプロバイダ310およびSAM3051~3051において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、EMDサービスセンタ302の秘密

鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、コンテンツプロバイダ301の権利書データ106およびサービスプロバイダ310のプライスタグデータ312を登録して権威化することも、EMDサービスセンタ302の認証機能によるものである。

また、EMDサービスセンタ302は、例えば、配信用鍵データKD1~KD。などの鍵データの管理を行なう鍵データ管理機能を有する。

また、EMDサービスセンタ302は、コンテンツプロバイダ301が登録した権利書データ106とSAM3051~SAM3054から入力した利用履歴データ308とサービスプロバイダ310が登録したプライスタグデータ312とに基づいて、ユーザホームネットワーク303のユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ301およびサービスプロバイダ310に分配して支払う権利処理(利益分配)機能を有する。

以下、コンテンツプロバイダ301の各構成要素について詳細に説明する。

[コンテンツプロバイダ301]

図50は、コンテンツプロバイダ301の機能プロック図であり、サービスプロバイダ310との間で送受信されるデータに関連するデータの流れが示されている。

図50に示すように、コンテンツプロバイダ301は、コンテンツマスタソースサーバ111、電子透かし情報付加部112、圧縮部113、暗号化部114、乱数発生部115、暗号化部116、署名処理部117、セキュアコンテナ作成部118、セキュアコンテナデータベース118a、記憶部119、相互認証部120、暗号化・復号部121、権利書データ作成部122、EMDサービスセンタ管理部125およびサービスプロバイダ管理部324を有する。

図50において、図2と同一符号を付した構成要素は、前述した第1実施形態 において図2および図3を参照しながら説明した同一符号の構成要素と同じであ

る。

すなわち、コンテンツプロバイダ301は、図2に示すSAM管理部124の 代わりにサービスプロバイダ管理部324を設けた構成をしている。

サービスプロバイダ管理部324は、セキュアコンテナ作成部118から入力したセキュアコンテナ104を、オフラインおよび/またはオンラインで、図49に示すサービスプロバイダ310に提供する。セキュアコンテナ104には、第1実施形態と同様に、図4A、図4B、図4Cに示すコンテンツファイルCFおよびその署名データSIG6, cpと、キーファイルKFおよびその署名データSIG7, cpと、公開鍵証明書データCERcpおよびその署名データSIG1, вsc とが格納されている。

サービスプロバイダ管理部324は、セキュアコンテナ104をオンラインでサービスプロバイダ310に配信する場合には、暗号化・復号部121においてセッション鍵データKsssを用いてセキュアコンテナ104を暗号化した後に、ネットワークを介してサービスプロバイダ310に配信する。

また、図3に示したコンテンツプロバイダ101内でのデータの流れは、サービスプロバイダ310にも同様に適用される。

[サービスプロバイダ310]

サービスプロバイダ310は、コンテンツプロバイダ301から提供を受けたセキュアコンテナ104内のコンテンツファイルCFおよびキーファイルKFと、自らが生成したプライスタグデータ312とを格納したセキュアコンテナ304を、オンラインおよび/またはオフラインで、ユーザホームネットワーク303のネットワーク機器3601およびAV機器3602~3604に配給する。

サービスプロバイダ310によるコンテンツ配給のサービス形態には、大きく 分けて、独立型サービスと連動型サービスとがある。

独立型サービスは、例えば、コンテンツを個別に配給するダウンロード専用の サービスである。また、連動型サービスは、番組、CM(広告)に連動してコン

テンツを配給するサービスであり、例えば、ドラマ番組のストリーム内にドラマ の主題歌や挿入歌のコンテンツが格納してある。ユーザは、ドラマ番組を見てい るときに、そのストリーム中にある主題歌や挿入歌のコンテンツを購入できる。

図51は、サービスプロバイダ310の機能プロック図である。

なお、図51には、コンテンツプロバイダ301から供給を受けたセキュアコンテナ104に応じたセキュアコンテナ304をユーザホームネットワーク30 3に供給する際のデータの流れが示されている。

図51に示すように、サービスプロバイダ310は、コンテンツプロバイダ管理部350、記憶部351、相互認証部352、暗号化・復号部353、署名処理部354、セキュアコンテナ作成部355、セキュアコンテナデータベース355a、プライスタグデータ作成部356、ユーザホームネットワーク管理部357、EMDサービスセンタ管理部358およびユーザ嗜好フィルタ生成部920を有する。

以下、コンテンツプロバイダ301から供給を受けたセキュアコンテナ104からセキュアコンテナ304を作成し、これをユーザホームネットワーク303に配給する際のサービスプロバイダ310内での処理の流れを図51および図52を参照しながら説明する。

図52は、当該処理のフローチャートである。

ステップSZ1:コンテンツプロバイダ管理部350は、オンラインおよび/ またはオフラインで、コンテンツプロバイダ301から図4に示すセキュアコン テナ104の供給を受けてセキュアコンテナ104を記憶部351に書き込む。

このとき、コンテンツプロバイダ管理部350は、オンラインの場合には、図50に示す相互認証部120と図51に示す相互認証部352との間の相互認証によって得られたセッション鍵データKsss を用いて、セキュアコンテナ104を暗号化・復号部353において復号した後に、記憶部351に書き込む。

ステップSZ2:署名処理部354において、記憶部351に記憶されている

セキュアコンテナ104の図4Cに示す署名データSIG1. BSC を、記憶部35 1から読み出したEMDサービスセンタ302の公開鍵データ KBSC, P を用いて 検証し、その正当性が認められた後に、図4Cに示す公開鍵証明書データCER cpから公開鍵データ Kcp, Pを取り出す。

ステップSZ3:署名処理部354は、当該取り出した公開鍵データKcp.pを 用いて、記憶部351に記憶されているセキュアコンテナ104の図4A、図4 Bに示す署名データSIGe.cp, SIG7.cpの検証を行う。

ステップSZ4:プライスタグデータ作成部356は、例えばコンテンツプロバイダ301からオフラインで通知されたコンテンツプロバイダ301が要求するコンテンツに対しての価格に、自らのサービスの価格を加算した価格を示すプライスタグデータ312を作成し、これをセキュアコンテナ作成部355に出力する。

ステップSZ5:署名処理部354は、コンテンツファイルCF、キーファイルKFおよびプライスタグデータ312のハッシュ値をとり、サービスプロバイダ310の秘密鍵データ $K_{SP,P}$ を用いて、署名データSIG $_{82,SP}$ ,SIG $_{84,SP}$ を作成し、これをセキュアコンテナ作成部355に出力する。

ステップSZ6:セキュアコンテナ作成部355は、図53A~図53Dに示すように、コンテンツファイルCFおよびその署名データSIGe2.sp と、キーファイルKFおよびその署名データSIGe3.Bscと、プライスタグデータ312およびその署名データSIGe4.sp と、公開鍵証明書データCERspおよびその署名データSIGe1.Bscとを格納したセキュアコンテナ304を作成し、セキュアコンテナデータベース355aに格納する。そして、セキュアコンテナ作成部355は、ユーザホームネットワーク303からの要求に応じたセキュアコンテナ304をセキュアコンテナテータベース355aから読み出してユーザホームネットワーク管理部357に出力する。

このとき、セキュアコンテナ304は、複数のコンテンツファイルCFと、そ

れらにそれぞれ対応した複数のキーファイルKFとを格納した複合コンテナであってもよい。例えば、単数のセキュアコンテナ304内に、それぞれ曲、ビデオクリップ、歌詞カード、ライナーノーツおよびジャケットに関する複数のコンテンツファイルCFを単数のセキュアコンテナ304に格納してもよい。これらの複数のコンテンツファイルCFなどは、ディレクトリー構造でセキュアコンテナ304内に格納してもよい。

また、セキュアコンテナ304は、デジタル放送で送信される場合には、MHEG(Multimedia and Hypermedia information coding Experts Group)プロトコルが用いられ、インターネットで送信される場合にはXML/SMIL/HTML(Hyper TextMarkup Language) プロトコルが用いられる。

このとき、コンテンツファイルCFおよびキーファイルKFは、コンテンツプロバイダ301によって一元的に管理され、セキュアコンテナ304を送信するプロトコルに依存しない。すなわち、コンテンツファイルCFおよびキーファイルKFは、MHEGおよびHTMLのプロトコルをトンネリングした形でセキュアコンテナ304内に格納される。

ステップSZ7:ユーザホームネットワーク管理部357は、セキュアコンテナ304を、オフラインおよび/またはオンラインでユーザホームネットワーク303に供給する。

ユーザホームネットワーク管理部357は、セキュアコンテナ304をオンラインでユーザホームネットワーク303のネットワーク機器3601に配信する場合には、相互認証後に、暗号化・復号部352においてセッション鍵データKss を用いてセキュアコンテナ304を暗号化した後に、ネットワークを介してネットワーク機器3601に配信する。

なお、ユーザホームネットワーク管理部357は、セキュアコンテナ304を 例えば衛星などを介して放送する場合には、セキュアコンテナ304をスクラン プル鍵データKscr を用いて暗号化する。また、スクランプル鍵データKscr を

ワーク鍵データ Kw を暗号化し、ワーク鍵データ Kw をマスタ鍵データ Ku を用いて暗号化する。

そして、ユーザホームネットワーク管理部 3 5 7 は、セキュアコンテナ 3 0 4 と共に、スクランプル鍵データ  $K_{SCR}$  およびワーク鍵データ  $K_{W}$  を、衛星を介してユーザホームネットワーク 3 0 3 に送信する。

また、例えば、マスタ鍵データ $K_M$  を、I C カードなどに記憶してオフラインでユーザホームネットワーク 3 0 3 に配給する。

また、ユーザホームネットワーク管理部357は、ユーザホームネットワーク 303から、当該サービスプロバイダ310が配給したコンテンツデータCに関 してのSP用購入履歴データ309を受信すると、これを記憶部351に書き込 む。

サービスプロバイダ310は、将来のサービス内容を決定する際に、SP用購入履歴データ309を参照する。また、ユーザ嗜好フィルタ生成部920は、SP用購入履歴データ309に基づいて、当該SP用購入履歴データ309を送信したSAM3051~3054のユーザの嗜好を分析してユーザ嗜好フィルタデータ900を生成し、これをユーザホームネットワーク管理部357を介してユーザホームネットワーク303のCAモジュール311に送信する。

図54には、サービスプロバイダ310内におけるEMDサービスセンタ30 2との間の通信に関連するデータの流れが示されている。

なお、以下に示す処理を行う前提として、サービスプロバイダ310の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、EMDサービスセンタ302に登録処理を行い、グローバルユニークな識別子SP\_IDを得ている。識別子SP\_IDは、記憶部351に記憶される。

先ず、サービスプロバイダ310が、EMDサービスセンタ302に、自らの 秘密鍵データKsp.sに対応する公開鍵データKsp.sの正当性を証明する公開鍵証

明書データCERspを要求する場合の処理を図54を参照しながら説明する。

先ず、サービスプロバイダ310は、真性乱数発生器を用いて乱数を発生して 秘密鍵データKsp.sを生成し、当該秘密鍵データKsp.sに対応する公開鍵データ Ksp.pを作成して記憶部351に記憶する。

EMDサービスセンタ管理部358、サービスプロバイダ310の識別子SP \_\_IDおよび公開鍵データKsp.pを記憶部351から読み出す。

そして、EMDサービスセンタ管理部358は、識別子SP\_IDおよび公開 鍵データKsp.pを、EMDサービスセンタ302に送信する。

そして、EMDサービスセンタ管理部 3 4 8 は、当該登録に応じて、公開鍵証明書データ  $CER_{SP}$  およびその署名データ  $SIG_{B1}$  BSC を EMD サービスセンタ 3 0 2 から入力して記憶部 3 5 1 に書き込む。

次に、サービスプロバイダ310が、EMDサービスセンタ302にプライスタグデータ312を登録して権威化する場合の処理を図54を参照して説明する

この場合には、署名処理部354において、プライスタグデータ作成部356が作成したプライスタグデータ312と記憶部351から読み出したグローバルュニークな識別子 $Content_ID$ とを格納したモジュール $Mod_{108}$  のハッシュ値が求められ、秘密鍵データ $K_{SP,S}$ を用いて署名データ $SIG_{80,SP}$  が生成される。

また、記憶部351から公開鍵証明書データCERspおよびその署名データS LG 81、ESCが読み出される。

そして、図55に示すプライスタグ登録要求用モジュールMod102を、相互認証部352とEMDサービスセンタ302との間の相互認証によって得られたセッション鍵データKsBsを用いて暗号化・復号部353において暗号化した後に、EMDサービスセンタ管理部358からEMDサービスセンタ302に送信する。

なお、モジュールModios に、サービスプロバイダ310のグローバルユニークな識別子SP\_IDを格納してもよい。

また、EMDサービスセンタ管理部358は、EMDサービスセンタ302から受信した決済レポートデータ307sを記憶部351に書き込む。

また、EMDサービスセンタ管理部358は、EMDサービスセンタ302から受信したマーケティング情報データ904を記憶部351に記憶する。

マーケティング情報データ 9 0 4 は、サービスプロバイダ 3 1 0 が今後配給するコンテンツデータ C を決定する際に参考にされる。

[EMDサービスセンタ302]

EMDサービスセンタ302は、前述したように、認証局 (CA:Certificate Authority)、鍵管理(Key Management)局および権利処理(Rights Clearing) 局としての役割を果たす。

図56は、EMDサービスセンタ302の機能の構成図である。

図56に示すように、EMDサービスセンタ302は、鍵サーバ141、鍵データベース141a、決済処理部442、署名処理部443、決算機関管理部144、証明書・権利書管理部445、CERデータベース445a、コンテンツプロバイダ管理部148、CPデータベース148a、SAM管理部149、SAMデータベース149a、相互認証部150、暗号化・復号部151、サービスプロバイダ管理部390、SPデータベース390a、ユーザ嗜好フィルタ生成部901およびマーケティング情報データ生成部902を有する。

図56において、図10および図11と同じ符号を付した機能プロックは、第 1実施形態で説明した同一符号の機能プロックと略同じ機能を有している。

以下、図56において、新たな符号を付した機能プロックについて説明する。 なお、図56には、EMDサービスセンタ302内の機能プロック相互間のデータの流れのうち、サービスプロバイダ310との間で送受信されるデータに関連するデータの流れが示されている。

また、図57には、EMDサービスセンタ302内の機能プロック相互間のデータの流れのうち、コンテンツプロバイダ301との間で送受信されるデータに関連するデータの流れが示されている。

また、図58には、EMDサービスセンタ302内の機能プロック相互間のデータの流れのうち、図49に示すSAM3051~3054 および決済機関91 との間で送受信されるデータに関連するデータの流れが示されている。

決算処理部 4.42は、図 5.8に示すように、SAM 3.0.51、 $\sim 3.0.5$ 1、から入力した利用履歴データ 3.0.82、証明書・権利書管理部 4.4.53 から入力した標準 小売価格データ SRP およびプライスタグデータ 3.1.22 に基づいて決済処理を行う。なお、この際に、決済処理部 4.4.22 は、サービスプロバイダ 3.1.02 によるダンピングの有無などを監視する。

決済処理部442は、決済処理により、図58に示すように、コンテンツプロバイダ301についての決済レポートデータ307cおよび決済請求権データ152cを作成し、これらをそれぞれコンテンツプロバイダ管理部148および決算機関管理部144に出力する。

また、決済処理により、図56および図58に示すように、サービスプロバイダ310についての決済レポートデータ307sおよび決済請求権データ152sを作成し、これらをそれぞれサービスプロバイダ管理部390および決算機関管理部144に出力する。

ここで、決済請求権データ152c, 152sは、当該データに基づいて、決済機関91に金銭の支払いを請求できる権威化されたデータである。

ここで、利用履歴データ308は、第1実施形態で説明した利用履歴データ108と同様に、セキュアコンテナ304に関連したラインセンス料の支払いを決定する際に用いられる。利用履歴データ308には、例えば、図59に示すように、セキュアコンテナ304に格納されたコンテンツデータCの識別子Content\_ID、セキュアコンテナ304に格納されたコンテンツデータCを提供

したコンテンツプロバイダ301の識別子CP\_ID、セキュアコンテナ304を配給したサービスプロバイダ310の識別子SP\_ID、コンテンツデータCの信号諸元データ、セキュアコンテナ304内のコンテンツデータCの圧縮方法、セキュアコンテナ304を記録した記録媒体の識別子Media\_ID、セキュアコンテナ304を配給を受けたSAM3051~305。の識別子SAM\_ID、当該SAM1051~105。のユーザのUSER\_IDなどが記述されている。従って、EMDサービスセンタ302は、コンテンツプロバイダ301およびサービスプロバイダ310の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク303のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータおよび決済請求権データを作成する。

証明書・権利書管理部445は、CERデータベース445aに登録されて権威化された公開鍵証明書データCERsp、公開鍵証明書データCERspおよび公開鍵証明書データCERsam1~CERsam2などを読み出すと共に、コンテンツプロバイダ301の権利書データ106およびコンテンツ鍵データKc、並びにサービスプロバイダ310のプライスタグデータ312などをCERデータベース45aに登録して権威化する。

このとき、証明書・権利書管理部445は、権利書データ106、コンテンツ 鍵データKcおよびプライスタグデータ312などのハッシュ値をとり、秘密鍵 データKgss を用いた署名データを付して権威化証明書データを作成する。

コンテンツプロバイダ管理部148は、コンテンツプロバイダ101との間で通信する機能を有し、登録されているコンテンツプロバイダ101の識別子CP \_\_IDなどを管理するCPデータベース148aにアクセスできる。

ユーザ嗜好フィルタ生成部901は、利用履歴データ308に基づいて、当該利用履歴データ308を送信したSAM3051~305』のユーザの嗜好に応

じたコンテンツデータCを選択するためのユーザ嗜好フィルタデータ903を生成し、ユーザ嗜好フィルタデータ903をSAM管理部149を介して、当該利用履歴データ308を送信したSAM3051~305。に送信する。

マーケティング情報データ生成部902は、利用履歴データ308に基づいて、例えば、複数のサービスプロバイダ310によってユーザホームネットワーク103に配給されたコンテンツデータCの全体の購入状況などを示すマーケティング情報データ904を生成し、これをサービスプロバイダ管理部390を介して、サービスプロバイダ310に送信する。サービスプロバイダ310は、マーケティング情報データ904を参考にして、今後提供するサービスの内容を決定する。

以下、EMDサービスセンタ302内での処理の流れを説明する。

EMDサービスセンタ302からコンテンツプロバイダ301への配信用鍵データ $KD_1 \sim KD_8$ の送信と、EMDサービスセンタ302から $SAM305_1 \sim 305_4$ への配信用鍵データ $KD_1 \sim KD_8$ の送信とは、第1実施形態の場合と同様に行なわれる。

また、EMDサービスセンタ302がコンテンツプロバイダ301から、公開 鍵証明書データの発行要求を受けた場合の処理も、証明書・権利書管理部445 がCERデータベース445aに対して登録を行なう点を除いて、前述した第1 実施形態の場合と同様に行なわれる。

以下、EMDサービスセンタ302がサービスプロバイダ310から、公開鍵証明書データの発行要求を受けた場合の処理を、図56および図60を参照しながら説明する。

図60は、当該処理のフローチャートである。

ステップSO1:サービスプロバイダ管理部390は、予めEMDサービスセンタ302によって与えられたサービスプロバイダ310の識別子SP\_ID、公開鍵データKsp, pおよび署名データSIG70. sp を含む公開鍵証明書データ登

録要求をサービスプロバイダ310から受信すると、これらを、相互認証部150と図51に示す相互認証部352と間の相互認証で得られたセッション鍵データKsssを用いて復号する。

ステップSO2: 当該復号した署名データSIG 70. SP の正当性を署名処理部443において確認した後に、識別子SP\_IDおよび公開鍵データ K SP. Pに基づいて、当該公開鍵証明書データの発行要求を出したサービスプロバイダ310がSPデータベース390aに登録されているか否かを確認する。

ステップSO3:証明書・権利書管理部445は、当該サービスプロバイダ310の公開鍵証明書データCERspをCERデータベース445 aから読み出してサービスプロバイダ管理部390に出力する。

ステップSO4:署名処理部443は、公開鍵証明書データCERspのハッシュ値をとり、EMDサービスセンタ302の秘密鍵データKBSC、s を用いて、署名データSIGs1.BSCを作成し、これをサービスプロバイダ管理部390に出力する。

ステップSO5:サービスプロバイダ管理部390は、公開鍵証明書データC ERsrおよびその署名データSIG®1. Bscを、相互認証部150と図51に示す相互認証部352と間の相互認証で得られたセッション鍵データKsBs を用いて暗号化した後に、サービスプロバイダ310に送信する。

なお、EMDサービスセンタ302が $SAM1051\sim105$ 。から、公開鍵証明書データの発行要求を受けた場合の処理は、第1実施形態と同様である。

また、EMDサービスセンタ302が、コンテンツプロバイダ301から権利 書データ106の登録要求を受けた場合の処理も、第1実施形態と同様である。

次に、EMDサービスセンタ302が、サービスプロバイダ310からプライスタグデータ312の登録要求を受けた場合の処理を、図56および図61を参照しながら説明する。

図61は、当該処理のフローチャートである。

ステップSP1:サービスプロバイダ管理部390がサービスプロバイダ310から図55に示すプライスタグ登録要求モジュール $Mod_{102}$ を受信すると、相互認証部150と図51に示す相互認証部352との間の相互認証で得られたセッション鍵データ $K_{SBS}$ を用いてプライスタグ登録要求モジュール $Mod_{102}$ を復号する。

ステップSP2:当該復号したプライスタグ登録要求モジュールMod102 に 格納された署名データSIG80, SP の正当性を署名処理部443において確認する。

ステップSP3:証明書・権利書管理部445は、プライスタグ登録要求モジュールMod<sub>102</sub> に格納されたプライスタグデータ312を、CERデータベース445aに登録して権威化する。

次に、EMDサービスセンタ302において決済を行なう場合の処理を図58 および図62を参照しながら説明する。

図62は、当該処理のフローチャートである。

ステップSQ1:SAM管理部149は、ユーザホームネットワーク303の例えばSAM3051から利用履歴データ308およびその署名データSIG205. SAM1を入力すると、利用履歴データ308および署名データSIG205. SAM1を、相互認証部150とSAM3051~3054との間の相互認証によって得られたセッション鍵データKSBSを用いて復号し、SAM3051の公開鍵データKSAM1. Fを用いて署名データSIG205. SAM1の検証を行なった後に、決算処理部442に出力する。

ステップSQ2:決済処理部442は、SAM3051から入力した利用履歴 データ308と、証明書・権利書管理部445から入力した標準小売価格データ SRPおよびプライスタグデータ312とに基づいて決済処理を行う。

決済処理部442は、決済処理により、図58に示すように、コンテンツプロバイダ301についての決済レポートデータ307cおよび決済請求権データ1

52cと、サービスプロバイダ310についての決済レポートデータ307sおよび決済請求権データ152sとを作成する。

なお、決済処理部 4 4 2 による決済処理は、利用履歴データ 3 0 8 を入力する 毎に行ってもよいし、所定の期間毎に行ってもよい。

ステップSQ3:図56および図58に示すように、コンテンツプロバイダ301およびサービスプロバイダ310についての決済請求権データ152c, 152sを作成し、これらを決算機関管理部144に出力する。

決算機関管理部144は、決済請求権データ152c, 152sと、それらについて秘密鍵データK<sub>BSC</sub>, s を用いて作成した署名データとを、相互認証およびセッション鍵データK<sub>SBS</sub> による復号を行なった後に、図49に示すペイメントゲートウェイ90を介して決済機関91に送信する。

これにより、決済請求権データ152cに示される金額の金銭がコンテンツプロバイダ301に支払われ、決済請求権データ152sに示される金額の金銭がサービスプロバイダ310に支払われる。

なお、EMDサービスセンタ302は、決済請求権データ152c, 152s をそれぞれコンテンツプロバイダ301およびサービスプロバイダ310に送信 してもよい。この場合には、コンテンツプロバイダ301およびサービスプロバ イダ310が、当該受信した決済請求権データ152c, 152sに基づいて決 済機関91に金銭を請求する。

ステップSQ4:コンテンツプロバイダ301およびサービスプロバイダ310についての決済レポートデータS307c, S307sが、それぞれコンテンツプロバイダ管理部148およびサービスプロバイダ管理部390を介して、コンテンツプロバイダ301およびサービスプロバイダ310に出力される。

EMDサービスセンタ302は、その他に、第1実施形態のEMDサービスセンタ102と同様に、SAM305 $_1$  ~305 $_4$  の出荷時の処理と、SAM登録リストの登録処理とを行なう。

[ユーザホームネットワーク303]

ューザホームネットワーク303は、図49に示すように、ネットワーク機器 3601 およびA/V機器3602  $\sim$ 3604 を有している。

ネットワーク機器 3601 は、CAモジュール 311 およびSAM3051 を内蔵している。また、AV機器 3602 ~ 3604 は、それぞれSAM3052 ~ 3054 を内蔵している。

SAM3051~3054の相互間は、例えば、1394シリアルインタフェースバスなどのバス191を介して接続されている。

なお、AV機器3602~360.は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス191を介してネットワーク機器3601のネットワーク通信機能を利用してもよい。

また、ユーザホームネットワーク303は、ネットワーク機能を有していない AV機器のみを有していてもよい。

以下、ネットワーク機器3601について説明する。

図63は、ネットワーク機器3601の構成図である。

図63に示すように、ネットワーク機器3601は、通信モジュール162、 CAモジュール311、復号モジュール905、SAM3051、復号・伸長モジュール163、購入・利用形態決定操作部165、ダウンロードメモリ167 、再生モジュール169および外部メモリ201を有する。

図63において、図16と同一符号を付した構成要素は、第1実施形態で説明 した同一符号の構成要素と同じである。

通信モジュール 1 6 2 は、サービスプロバイダ 3 1 0 との間の通信処理を行なう。

具体的には、通信モジュール162は、サービスプロバイダ310から衛星放送などで受信したセキュアコンテナ304を復号モジュール905に出力する。また、通信モジュール162は、サービスプロバイダ310に電話回線などを介

してSP用購入履歴データ309を受信したユーザ嗜好フィルタデータ900を CAモジュール311に出力すると共に、CAモジュール311から入力したS P用購入履歴データ309を電話回線などを介してサービスプロバイダ310に 送信する。

図64は、CAモジュール311および復号モジュール905の機能プロック 図である。

図64に示すように、CAモジュール311は、相互認証部906、記憶部907、暗号化・復号部908およびSP用購入履歴データ生成部909を有する

相互認証部 8 0 6 は、CAモジュール 3 1 1 とサービスプロバイダ 3 1 0 との間で電話回線を介してデータを送受信する際に、サービスプロバイダ 3 1 0 との間で相互認証を行ってセッション鍵データ K<sub>SBS</sub> を生成し、これを暗号化・復号部 9 0 8 に出力する。

記憶部907は、例えば、サービスプロバイダ310とユーザとの間で契約が成立した後に、サービスプロバイダ310からICカード912などを用いてオフラインで供給されたマスタ鍵データ K M を記憶する。

暗号化・復号部908は、復号モジュール905の復号部910からそれぞれ暗号化されたスクランブル鍵データ $K_{SCR}$  およびワーク鍵データ $K_w$  を入力し、記憶部907から読み出したマスタ鍵データ $K_M$  を用いてワーク鍵データ $K_W$  を復号する。そして、暗号化・復号部908は、当該復号したワーク鍵データ $K_W$  を用いてスクランブル鍵データ $K_{SCR}$  を復号部910に出力する。

また、暗号化・復号部908は、電話回線などを介して通信モジュール162 がサービスプロバイダ310から受信したユーザ嗜好フィルタデータ900を、 相互認証部906からのセッション鍵データKsBs を用いて復号して復号モジュ ール905のセキュアコンテナ選択部911に出力する。

また、暗号化・復号部908は、SP用購入履歴データ生成部909から入力したSP用購入履歴データ309を、相互認証部906からのセッション鍵データKsss を用いて復号して通信モジュール162を介してサービスプロバイダ310に送信する。

SP用購入履歴データ生成部909は、図63に示す購入・利用形態決定操作部165を用いてユーザによるコンテンツデータCの購入操作に応じた操作信号S165、またはSAM3051からの利用制御状態データ166に基づいて、サービスプロバイダ310に固有のコンテンツデータCの購入履歴を示すSP用購入履歴データ309を生成し、これを暗号化・復号部908に出力する。

SP用購入履歴データ309は、例えば、サービスプロバイダ310が配信サービスに関してユーザから徴収したい情報、月々の基本料金(ネットワーク家賃)、契約(更新)情報および購入履歴情報などを含む。

なお、CAモジュール311は、サービスプロバイダ310が課金機能を有している場合には、サービスプロバイダ310の課金データベース、顧客管理データベースおよびマーケティング情報データベースと通信を行う。この場合に、CAモジュール311は、コンテンツデータの配信サービスについての課金データをサービスプロバイダ310に送信する。

復号モジュール 9 0 5 は、復号部 9 1 0 およびセキュアコンテナ選択部 9 1 1 を有する。

復号部 9 1 0 は、通信モジュール 1 6 2 から、それぞれ暗号化されたセキュアコンテナ 3 0 4、スクランプル鍵データ $K_{SCR}$  およびワーク鍵データ $K_{W}$  を入力する。

そして、復号部 9 1 0 は、暗号化されたスクランブル鍵データ  $K_{scr}$  およびワーク鍵データ  $K_w$  を C A モジュール 3 1 1 の暗号化・復号部 9 0 8 に出力し、暗号化・復号部 9 0 8 から復号されたスクランブル鍵データ  $K_{scr}$  を入力する。

そして、復号部910は、暗号化されたセキュアコンテナ304を、スクラン

ブル鍵データKscr を用いて復号した後に、セキュアコンテナ選択部911に出力する。

なお、セキュアコンテナ304が、MPEG2 Transport Stream 方式でサービスプロバイダ310から送信される場合には、例えば、復号部910は、TS Packet 内のECM(Entitlement Control Message) からスクランブル鍵データKscrを取り出し、EMM(Entitlement Management Message)からワーク鍵データKwを取り出す。

ECMには、その他に、例えば、チャンネル毎の番組属性情報などが含まれている。また、EMMは、その他に、ユーザ(視聴者)毎に異なる個別試聴契約情報などが含まれている。

セキュアコンテナ選択部 9 1 1 は、復号部 9 1 0 から入力したセキュアコンテナ 3 0 4 を、CAモジュール 3 1 1 から入力したユーザ嗜好フィルタデータ 9 0 0 を用いてフィルタリング処理して、ユーザの嗜好に応じたセキュアコンテナ 3 0 4 を選択してSAM 3 0 5 1 に出力する。

次に、SAM3051について説明する。

なお、SAM3051は、サービスプロバイダ310についての署名検証処理を行なうなど、コンテンツプロバイダ301に加えてサービスプロバイダ310に関しての処理を行う点を除いて、図17~図41を用いて前述した第1実施形態のSAM1051と基本的に行なう機能および構造を有している。

また、SAM3052~3054は、SAM3051と基本的に同じ機能を有している。

すなわち、 $SAM3051 \sim 3051$ は、コンテンツ単位の課金処理をおこなうモジュールであり、EMDサービスセンタ302との間で通信を行う。

以下、SAM3051の機能について詳細に説明する。

図65は、SAM3051の機能の構成図である。

なお、図65には、サービスプロバイダ310からセキュアコンテナ304を

入力し、セキュアコンテナ304内のキーファイルKFを復号する処理に関連するデータの流れが示されている。

図65に示すように、SAM3051は、相互認証部170、暗号化・復号部171,172,173、誤り訂正部181、ダウンロードメモリ管理部182、セキュアコンテナ復号部183、復号・伸長モジュール管理部184、EMDサービスセンタ管理部185、利用監視部186、署名処理部189、SAM管理部190、記憶部192、メディアSAM管理部197、スタックメモリ200、サービスプロバイダ管理部580、課金処理部587、署名処理部598および外部メモリ管理部811を有する。

なお、図65に示すSAM3051の所定の機能は、SAM1051の場合と 同様に、CPUにおいて秘密プログラムを実行することによって実現される。

図65において、図17と同じ符号を付した機能プロックは、第1実施形態で 説明した同一符号の機能プロックと同じである。

また、図63に示す外部メモリ201には、第1実施形態で説明した処理および後述する処理を経て、利用履歴データ308およびSAM登録リストが記憶される。

また、スタックメモリ200には、図66に示すように、コンテンツ鍵データ Kc、権利書データ(UCP)106、記憶部192のロック鍵データ $K_{LOC}$ 、コンテンツプロバイダ301の公開鍵証明書データ $CER_{CP}$ 、サービスプロバイダ310の公開鍵証明書データ $CER_{SP}$ 、利用制御状態データ(UCS)366、SAMプログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_3$  およびプライスタグデータ312などが記憶される。

以下、SAM3051の機能プロックのうち、図65において新たに符号を付した機能プロックについて説明する。

署名処理部589は、記憶部192あるいはスタックメモリ200から読み出したEMDサービスセンタ302の公開鍵データK<sub>BSC.P</sub>、コンテンツプロバイ

ダ301の公開鍵データK<sub>sp.p</sub>およびサービスプロバイダ310の公開鍵データ K<sub>sp.p</sub>を用いて、セキュアコンテナ304内の署名データの検証を行なう。

課金処理部587は、図67に示すように、図63に示す購入・利用形態決定 操作部165からの操作信号S165と、スタックメモリ200から読み出され たプライスタグデータ312とに基づいて、ユーザによるコンテンツの購入・利 用形態に応じた課金処理を行う。

課金処理部587による課金処理は、利用監視部186の監視の下、権利書データ106が示す使用許諾条件などの権利内容および利用制御状態データ166 に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行うことができる。

また、課金処理部587は、課金処理において、利用履歴データ308を生成し、これを外部メモリ管理部811を介して外部メモリ201に書き込む。

ここで、利用履歴データ308は、第1実施形態の利用履歴データ108と同様に、EMDサービスセンタ302において、セキュアコンテナ304に関連したラインセンス料の支払いを決定する際に用いられる。

また、課金処理部587は、操作信号S165に基づいて、ユーザによるコンテンツの購入・利用形態を記述した利用制御状態(UCS: Usage Control Status)データ166を生成し、これを外部メモリ管理部811を介して外部メモリ201に書き込む。

コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。

ここで、利用制御状態データ166は、ユーザがコンテンツの購入形態を決定 したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユー ザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御 状態データ166には、コンテンツのID、購入形態、買い切り価格、当該コン

テンツの購入が行なわれた $SAMOSAM_ID$ , 購入を行なったユーザのUSER IDなどが記述されている。

なお、決定された購入形態が再生課金である場合には、例えば、SAM305 1 からサービスプロバイダ310に利用制御状態データ166をリアルタイムに 送信し、サービスプロバイダ310がEMDサービスセンタ302に、利用履歴 データ108をSAM1051に取りにいくことを指示する。

また、決定された購入形態が買い切りである場合には、例えば、利用制御状態 データ166が、サービスプロバイダ310およびEMDサービスセンタ302 にリアルタイムに送信される。

また、SAM3051では、EMDサービスセンタ管理部185がEMDサービスセンタ302から受信したユーザ嗜好フィルタデータ903が、サービスプロバイダ管理部580に出力される。そして、サービスプロバイダ管理部580において、図63に示す復号モジュール905から入力したセキュアコンテナ304が、ユーザ嗜好フィルタデータ903に基づいてフィルタリングされてユーザの嗜好に応じたセキュアコンテナ304が選択され、当該選択されたセキュアコンテナ304が誤り訂正部181に出力される。これにより、SAM3051において、当該SAM3051のユーザが契約している全てのサービスプロバイダ310を対象として、当該ユーザによるコンテンツデータCの購入状況から得られた当該ユーザの嗜好に基づいたコンテンツデータCの選択処理が可能になる

以下、SAM3051内での処理の流れを説明する。

EMDサービスセンタ302から受信した配信用鍵データKD: ~KDs を記憶部192に格納する際のSAM305: 内での処理の流れは、前述したSAM105: の場合と同様である。

以下、セキュアコンテナ304をサービスプロバイダ310から入力し、セキュアコンテナ304内のキーファイルKFを復号する際のSAM3051内での

処理の流れを図65および図68を参照しながら説明する。

図68は、当該処理のフローチャートである。

ステップSR1:相互認証部170と図51に示すサービスプロバイダ310の相互認証部352との間で相互認証が行なわれる。

暗号化・復号部171は、当該相互認証によって得られたセッション鍵データ Ksss を用いて、サービスプロバイダ管理部580を介してサービスプロバイダ 310から受信した図53A~図53Dに示すセキュアコンテナ304を復号する。

ステップSR2:署名処理部589は、図53Dに示す署名データSIG $_{81,8}$   $_{8c}$ の検証を行なった後に、図53Dに示す公開鍵証明書データCER $_{8p}$ 内に格納されたサービスプロバイダ310の公開鍵データK $_{8p,p}$ を用いて、署名データSIG $_{82,8p}$ , SIG $_{83,8p}$ , SIG $_{84,8p}$  の正当性を確認する。

サービスプロバイダ管理部 5 8 0 は、署名データ S I G e 2, sp , S I G e 3, sp , S I G e 4, sp の正当性が確認されると、セキュアコンテナ 3 0 4 を誤り訂正部 1 8 1 に出力する。

誤り訂正部181は、セキュアコンテナ304を誤り訂正した後に、ダウンロードメモリ管理部182に出力する。

ステップSR3:ダウンロードメモリ管理部182は、相互認証部170と図63に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ304をダウンロードメモリ167に書き込む。

ステップSR4:ダウンロードメモリ管理部182は、相互認証部170と図63に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ304に格納された図53Bに示すキーファイルKFを読み出してセキュアコンテナ復号部183に出力する。

そして、セキュアコンテナ復号部183は、記憶部192から入力した対応する期間の配信用鍵データKD1~KDsを用いて、キーファイルKFを復号する

ステップSR5:セキュアコンテナ復号部183は、図53Bに示す署名・証明書モジュールMod1 に格納された署名データSIG1. BSC、SIG2. cp~SIG4. cpを署名処理部589に出力する。

ステップSR6:セキュアコンテナ復号部183は、署名データSIG2、 $\varepsilon_P$  ~ SIG4、 $\varepsilon_P$  の正当性が確認されると、キーファイルKFをスタックメモリ200 に書き込む。

以下、サービスプロバイダ3 1 0 からダウンロードメモリ 1 6 7 にダウンロードされたセキュアコンテナ 3 0 4 の購入形態を決定するまでの処理の流れを図 6 7 および図 6 9 を参照しながら説明する。

図69は、当該処理のフローチャートである。

ステップSS1:課金処理部587において、ユーザによる図63に示す購入・利用形態決定操作部165の操作によって、試聴モードを示す操作信号S165が入力されたか否かが判断あれ、入力されたと判断された場合にはステップSS2の処理が実行される

ステップSS2:例えば、ダウンロードメモリ167に記憶されているコンテンツファイルCFが、復号・伸長モジュール管理部184を介して、図63に示す復号・伸長モジュール163に出力される。

このとき、コンテンツファイルCFに対して、相互認証部170とメディアS AM167aとの間の相互認証およびセッション鍵データ Kses による暗号化・復号と、相互認証部170と相互認証部220との間の相互認証およびセッション鍵データ Kses による暗号化・復号とが行なわれる。

コンテンツファイルCFは、図63に示す復号部221において復号された後に、復号部222に出力される。

また、スタックメモリ200から読み出されたコンテンツ鍵データKcおよび 半開示パラメータデータ199が、図63に示す復号・伸長モジュール163に 出力される。このとき、相互認証部170と相互認証部220との間の相互認証 後に、コンテンツ鍵データKcおよび半開示パラメータデータ199に対してセ ッション鍵データKsss による暗号化および復号が行なわれる。

次に、復号された半開示パラメータデータ199が半開示処理部225に出力され、半開示処理部225からの制御によって、復号部222によるコンテンツ鍵データKcを用いたコンテンツデータCの復号が半開示で行われる。

次に、半開示で復号されたコンテンツデータCが、伸長部223において伸長された後に、電子透かし情報処理部224に出力される。

次に、電子透かし情報処理部224においてユーザ電子透かし情報用データ196がコンテンツデータCに埋め込まれた後、コンテンツデータCが再生モジュール169において再生され、コンテンツデータCに応じた音響が出力される。

ステップSS3:コンテンツを試聴したユーザが、購入・利用形態決定操作部 165を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号 S165が課金処理部187に出力される。

ステップSS4:課金処理部187において、決定された購入形態に応じた利用履歴データ308および利用制御状態データ166が生成され、利用履歴データ308が外部メモリ管理部811を介して外部メモリ201に書き込まれると共に利用制御状態データ166がスタックメモリ200に書き込まれる。

以後は、利用監視部186において、利用制御状態データ166によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御(監視)される。

ステップSS5:スタックメモリ200に格納されているキーファイルKFに

、利用制御状態データ166が加えられ、購入形態が決定した後述する図71に示す新たなキーファイルKF11が生成される。キーファイルKF11は、スタックメモリ200に記憶される。

図71に示すように、キーファイル $KF_1$  に格納された利用制御状態データ166はストレージ鍵データ $K_{STR}$  を用いてDESのCBCモードを利用して暗号化されている。また、当該ストレージ鍵データ $K_{STR}$  をMAC鍵データとして用いて生成したMAC値であるMACsoo が付されている。また、利用制御状態データ166およびMACsoo からなるモジュールは、メディア鍵データMBD を用いてDESのCBCモードを利用して暗号化されている。また、当該モジュールには、当該メディア鍵データ $K_{MBD}$  をMAC鍵データとして用いて生成したMAC値である $MACsool}$  が付されている。

次に、ダウンロードメモリ167に記憶されている購入形態が既に決定された コンテンツデータCを再生する場合の処理の流れを、図67および図70を参照 しながら説明する。

図70は、当該処理のフローチャートである。

ステップST1:例えば、ユーザによる操作に応じて、再生対象となるコンテンツの指定をSAMが受ける。

ステップST2:利用監視部186の監視下で、操作信号S165に基づいて、ダウンロードメモリ167に記憶されているコンテンツファイルCFが読み出される。

ステップST3:当該読み出されたコンテンツファイルCFが、図63に示す 復号・伸長モジュール163に出力される。

また、スタックメモリ200から読み出されたコンテンツ鍵データKcが復号・伸長モジュール163に出力される。

ステップST4:復号・伸長モジュール163の復号部222において、コンテンツ鍵データKcを用いたコンテンツファイルCFの復号と、伸長部223に

よる伸長処理とが行なわれ、再生モジュール169において、コンテンツデータ Cが再生される。

ステップST5:課金処理部587において、操作信号S165に応じて、利用履歴データ308が更新される。

利用履歴データ308は、秘密鍵データ $K_{SAM1.S}$ を用いて作成したそれぞれ署名データ $SIG_{205.SAM1}$ と共に、EMDサービスセンタ管理部185を介して、所定のタイミングで、EMDサービスセンタ302に送信される。

以下、図72に示すように、例えば、ネットワーク機器3601のダウンロードメモリ167にダウンロードされた既に購入形態が決定されたコンテンツファイルCFを、バス191を介して、AV機器3602のSAM3052に転送する場合のSAM3051内での処理の流れを図73および図74を参照しながら説明する。

ステップSU1:ユーザは、購入・利用形態決定操作部165を操作して、ダウンロードメモリ167に記憶された所定のコンテンツをAV機器360 $_2$ に転送することを指示し、当該操作に応じた操作信号S165が、課金処理部587に出力される。

これにより、課金処理部587は、操作信号S165に基づいて、スタックメモリ200に記憶されている利用履歴データ308を更新する。

ステップSU2:ダウンロードメモリ管理部182は、ダウンロードメモリ167から読み出した図75Aに示すコンテンツファイルCFをSAM管理部180に出力する。

ステップSU3:スタックメモリ200から読み出した図75Bに示す既に購入形態が決定されたキーファイルKF11を、署名処理部589およびSAM管理部190に出力する。

ステップSU4:署名処理部589は、キーファイルKF11の署名データSI Gao. SAM1 を作成し、これをSAM管理部190に出力する。

ステップSU5:SAM管理部190は、記憶部192から、図75Cに示す 公開鍵証明書データCER<sub>SAM1</sub>およびその署名データSIG<sub>22, BSC</sub>を読み出す。

また、相互認証部170は、SAM3052との間で相互認証を行って得たセッション鍵データKsesを暗号化・復号部171に出力する。

SAM管理部190は、図75A, B, Cに示すデータからなるセキュアコンテナを作成する。

ステップSU6:暗号化・復号部171において、セッション鍵データKsgsを用いて当該セキュアコンテナを暗号化して作成して、図73に示すAV機器3602のSAM3052に出力する。

以下、図72に示すように、SAM3051から入力したコンテンツファイル CFなどを、RAM型などの記録媒体(メディア)に書き込む際のSAM305 2内での処理の流れを、図76および図77を参照しながら説明する。

図77は、当該処理のフローチャートである。

ステップSV1:SAM3052のSAM管理部190は、図76に示すように、図75Aに示すコンテンツファイルCF、図75Bに示すキーファイルKF11およびその署名データSIG80, SAM1 と、図75Cに示す公開鍵署名データCERSAM1およびその署名データSIG22, BSCとを、ネットワーク機器3601のSAM3051から入力する。

そして、暗号化・復号部171において、SAM管理部190が入力したコンテンツファイルCFと、キーファイル $KF_{11}$ およびその署名データ $SIG_{80,SAM}$ 1、と、公開鍵署名データ $CER_{SAM1}$ およびその署名データ $SIG_{22,BSC}$ とが、相互認証部170と $SAM305_1$  の相互認証部170との間の相互認証によって得られたセッション鍵データ $K_{SBS}$  を用いて復号される。

次に、セッション鍵データKsss を用いて復号されたコンテンツファイルCF がメディアSAM管理部197に出力される。

また、セッション鍵データKsBs を用いて復号されたキーファイルKF11およ

びその署名データSIG80, 8AM1 と、公開鍵署名データCER8AM1およびその署名データSIG22, 88cとが、スタックメモリ 2 0 0 に書き込まれる。

ステップSV2:署名処理部589は、スタックメモリ200から読み出した 署名データSIG<sub>22, BSC</sub>を、記憶部192から読み出した公開鍵データK<sub>BSC, P</sub> を用いて検証して、公開鍵証明書データCER<sub>SAM1</sub>の正当性を確認する。

そして、署名処理部589は、公開鍵証明書データCERsam1の正当性を確認すると、公開鍵証明書データCERsam1に格納された公開鍵データKsam1、pを用いて、署名データSIG80、sam1の正当性を確認する。

ステップSV3:署名データSI $G_{80, SAM1}$  の正当性を確認されると、図75 Bに示すキーファイル $KF_{11}$ をスタックメモリ200から読み出して暗号化・復号部173に出力する。

そして、暗号化・復号部173は、記憶部192から読み出した記録用鍵データ $K_{STR}$ 、メディア鍵データ $K_{MBD}$  および購入者鍵データ $K_{PIN}$  を用いてキーファイル $KF_{11}$ を順に暗号化してメディアSAM管理部197に出力する。

ステップSV4:メディアSAM管理部197は、SAM管理部190から入力したコンテンツファイルCFおよび暗号化・復号部173から入力したキーファイルKF11を、図72に示す記録モジュール260に出力する。

そして、記録モジュール 260 は、メディア SAM 管理部 197 から入力した コンテンツファイル CF およびキーファイル  $KF_{11}$  を、 図72 に示す RAM 型の 記録媒体 250 の RAM 領域 251 に書き込む。

なお、SAM3051内での処理のうち、コンテンツの購入形態が未決定のROM型の記録媒体の購入形態を決定する際のAV機器3602内での処理の流れ、AV機器360%において購入形態が未決定のROM型の記録媒体からセキュアコンテナ304を読み出してこれをAV機器360%に転送してRAM型の記録媒体に書き込む際の処理の流れは、サービスプロバイダ310の秘密鍵データを用いた署名データの署名データの検証を行なう点と、購入形態を決定したキー

ファイル内にプライスタグデータ312を格納する点を除いて、第1実施形態の SAM1051の場合と同じである。

次に、図49に示すEMDシステム300の全体動作について説明する。

図78および図79は、EMDシステム300の全体動作のフローチャートである。

ここでは、サービスプロバイダ310からユーザホームネットワーク303に オンラインでセキュアコンテナ304を送信する場合を例示して説明する。

なお、以下に示す処理の前提として、EMDサービスセンタ302へのコンテンツプロバイダ301、サービスプロバイダ310およびSAM3051~30 54の登録は既に終了しているものとする。

ステップS 2 1:E M D サービスセンタ 3 0 2 は、コンテンツプロバイダ 3 0 1 の公開鍵データ  $K_{CP,P}$  の公開鍵証明書  $C \to R_{CP}$  を、自らの署名データ  $S \to R_{CP}$  と共にコンテンツプロバイダ 3 0 1 に送信する。

また、EMDサービスセンタ302は、コンテンツプロバイダ301の公開鍵 データ $K_{SP,P}$ の公開鍵証明書 $CER_{SP}$ を、自らの署名データ $SIG_{B1,BSC}$ と共に サービスプロバイダ310に送信する。

また、EMDサービスセンタ302は、各々有効期限が1カ月の6カ月分の配信用鍵データKD1~KDs をコンテンツプロバイダ301に送信し、3カ月分の配信用鍵データKD1~KDs をユーザホームネットワーク303のSAM3051~3054 に送信する。

ステップS22:コンテンツプロバイダ301は、図7Aに示す権利登録要求 モジュールMod2を、EMDサービスセンタ302に送信する。

そして、EMDサービスセンタ302は、所定の署名検証を行った後に、権利 書データ106およびコンテンツ鍵データKcを登録して権威化(認証)する。

ステップS23:コンテンツプロバイダ301は、署名データの作成処理や、 SIG対応する期間の配信用鍵データKD: ~KD: などを用いた暗号化処理を

経て、図4A、図4B、図4Cに示すデータを格納したセキュアコンテナ104 を、サービスプロバイダ310に供給する。

ステップS 2 4:サービスプロバイダ 3 1 0 は、図 4 Cに示す署名データS I  $G_{1. BSC}$  を検証した後に、公開鍵証明書データ C E  $R_{CP. P}$  C E  $R_{CP. P}$  E

ステップS25:サービスプロバイダ310は、プライスタグデータ312を 作成し、プライスタグデータ312を格納した図53に示すセキュアコンテナ3 04を作成する。

ステップS 2 6:サービスプロバイダ 3 1 0 は、図 5 5 に示すプライスタグ登録要求モジュールM 0 d 102 を、E M D サービスセンタ 3 0 2 に送信する。

そして、EMDサービスセンタ302は、所定の署名検証を行った後に、プライスタグデータ312を登録して権威化する。

ステップS27:サービスプロバイダ310は、例えば、ユーザホームネットワーク303のCAモジュール311からの要求に応じて、ステップS25で作成したセキュアコンテナ304を、オンラインあるいはオフラインで、図63に示すネットワーク機器3601の復号モジュール905に送信する。

ステップS28:CAモジュール311は、SP用購入履歴データ309を作成し、これを所定のタイミングで、サービスプロバイダ310に送信する。

ステップS30:SAM3051~3054のいずれかにおいて、配信用鍵デ

ータ $KD_1 \sim KD_s$  を用いて、図53Bに示すキーファイルKFを復号する。そして、 $SAM305_1 \sim 305_4$  のいずれかにおいて、図53Bに示す署名データ $SIG_{1,BSC}$  を検証した後に、公開鍵証明書データ $CER_{CP}$ に格納された公開鍵データ $K_{CP,P}$ を用いて、図53Bに示す署名データ $SIG_{2,CP}$ ,  $SIG_{3,CP}$  および $SIG_{4,CP}$ を検証して、コンテンツデータC、コンテンツ鍵データ $K_{C}$  なおよび権利書データ106が正当なコンテンツプロバイダ301によって作成されたものであるかを確認する。

ステップS31:ユーザが図63の購入・利用形態決定操作部165を操作してコンテンツの購入・利用形態を決定する。

ステップS32:ステップS31において生成された操作信号S165に基づいて、SAM305 $_1$  ~305 $_4$  において、セキュアコンテナ304の利用履歴 (Usage Log) データ308が生成される。

SAM3051~3054からEMDサービスセンタ302に、利用履歴データ308およびその署名データSIG205, SAM1が送信される。

EMDサービスセンタ302は、利用履歴データ308に基づいて、コンテンツプロバイダ301およびサービスプロバイダ310の各々について、課金内容を決定(計算)し、その結果に基づいて、決済請求権データ152c, 152sを作成する。

EMDサービスセンタ302は、ペイメントゲートウェイ90を介して決済機関91に、決済請求権データ152c, 152sを自らの署名データと共に送信し、これにより、ユーザホームネットワーク303のユーザが決済機関91に支払った金銭が、コンテンツプロバイダ301およびサービスプロバイダ310の所有者に分配される。

以上説明したように、EMDシステム300では、図4に示すフォーマットの セキュアコンテナ104をコンテンツプロバイダ301からサービスプロバイダ 310に配給し、セキュアコンテナ104内のコンテンツファイルCFおよびキ

ーファイルKFをそのまま格納したセキュアコンテナ304をサービスプロバイダ310からユーザホームネットワーク303に配給し、キーファイルKFについての処理を $SAM3051\sim305$ 。内で行う。

また、キーファイルKFに格納されたコンテンツ鍵データKcおよび権利書データ106は、配信鍵データKD1 $\sim$ KDsを用いて暗号化されており、配信鍵データKD1 $\sim$ KDsを保持しているSAM3051 $\sim$ 305。内でのみ復号される。そして、SAM3051 $\sim$ 305。では、耐タンパ性を有するモジュールであり、権利書データ106に記述されたコンテンツデータCの取り扱い内容に基づいて、コンテンツデータCの購入形態および利用形態が決定される。

従って、EMDシステム300によれば、ユーザホームネットワーク303におけるコンテンツデータCの購入および利用を、サービスプロバイダ310における処理とは無関係に、コンテンツプロバイダ101の関係者が作成した権利書データ106の内容に基づいて確実に行わせることができる。すなわち、EMDシステム300にれば、権利書データ106をサービスプロバイダ310が管理できないようできる。

そのため、EMDシステム300によれば、異系列の複数のサービスプロバイダ310を介してユーザホームネットワーク303にコンテンツデータCが配給された場合でも、ユーザホームネットワーク303における当該コンテンツデータCについての権利処理を、コンテンツプロバイダ301が作成した共通の権利書データ106に基づいて行わせることができる。

また、EMDシステム 3 0 0 では、サービスプロバイダ 3 1 0 からユーザホームネットワーク 1 0 3 へのコンテンツデータ C の配給を、オンラインおよびオフラインの何れの場合でもセキュアコンテナ 3 0 4 を用いて行うことで、双方の場合において、SAM 3 0 5 1  $\sim$  3 0 5 2 におけるコンテンツデータ C の権利処理を共通化できる。

また、EMDシステム300では、ユーザホームネットワーク303内のネッ

トワーク機器3601 およびAV機器3602 ~360 においてコンテンツデータCを購入、利用、記録および転送する際に、常に権利書データ106に基づいて処理を行うことで、共通の権利処理ルールを採用できる。

また、EMDシステム300によれば、EMDサービスセンタ302が、認証機能、鍵データ管理機能および権利処理(利益分配)機能を有することから、コンテンツの利用に伴ってユーザが支払った金額が、コンテンツプロバイダ301 およびEMDサービスセンタ302の所有者に、予め決められた比率に従って確実に分配される。

また、EMDシステム300によれば、同じコンテンツプロバイダ301が供給した同じコンテンツファイルCFについての権利書データ106は、サービスプロバイダ310のサービス形態とは無関係に、そのまま $SAM3051\sim30$ 5。に供給される。従って、 $SAM3051\sim305$ 。において、権利書データ106に基づいて、コンテンツプロバイダ301の意向通りに、コンテンツファイルCFの利用を行わせることができる。

すなわち、EMDシステム300によれば、コンテンツを用いたサービスおよびユーザによるコンテンツの利用が行われる際に、従来のように監査組織725に頼ることなく、技術的な手段によって、コンテンツプロバイダ301の所有者の権利および利益を確実に守ることができる。

#### 第2実施形態の第1変形例

図80は、第2実施形態の第1変形例に係わる2個のサービスプロバイダを用いたEMDシステム300aの構成図である。

図80において、図49と同一符号を付した構成要素は、第2実施形態で説明 した同一符号の構成要素と同じである。

図80に示すように、EMDシステム300aでは、コンテンツプロバイダ301からサービスプロバイダ310aおよび310bに、同じセキュアコンテナ104を供給する。

サービスプロバイダ310aは、例えば、コンテンツをドラマ番組の提供サービスを行っており、当該サービスにおいて、当該ドラマ番組に関連するコンテンツデータCと、当該コンテンツデータCについて独自に作成したプライスタグデータ312aとを格納したセキュアコンテナ304aを作成し、これをネットワーク機器3601に配給する。

また、サービスプロバイダ310bは、例えば、カラオケサービスを提供しており、当該サービスにおいて、当該カラオケサービスに関連するコンテンツデータCと、当該コンテンツデータCについて独自に作成したプライスタグデータ312bとを格納したセキュアコンテナ304bを作成し、これをネットワーク機器3601に配給する。

ここで、セキュアコンテナ304a, 304bのフォーマットは、図53を用いた説明したセキュアコンテナ304と同じである。

ネットワーク機器360a1には、サービスプロバイダ310a, 310bの 各々に対応したCAモジュール311a, 311bが設けられている。

次に、CAモジュール311a,311bは、配給されたセキュアコンテナ304a,304bに応じたSP用購入履歴データ309a,309bをそれぞれ作成し、これらをそれぞれサービスプロバイダ310a,310bに送信する。また、CAモジュール311a,311bは、セキュアコンテナ304a,3

04bをセッション鍵データKsss で復号した後に、SAM3051~3054 に出力する。

次に、SAM3051~~305。において、共通の配信用鍵データKD1~~K Ds を用いて、セキュアコンテナ304a, 304b内のキーファイルKFが復号され、共通の権利書データ106に基づいて、ユーザからの操作に応じたコン

テンツの購入・利用に関する処理が行われ、それに応じた利用履歴データ308 が作成される。

そして、 $SAM3051\sim305$ 4からEMDサービスセンタ302に、利用履歴データ308が送信される。

EMDサービスセンタ302では、利用履歴データ308に基づいて、コンテンツプロバイダ301およびサービスプロバイダ310a,310bの各々について、課金内容を決定(計算)し、その結果に基づいて、それぞれに対応する決済請求権データ152c,152sa,152sbを作成する。

EMDサービスセンタ302は、ペイメントゲートウェイ90を介して決済機関91に、決済請求権データ152c, 152sa, 152sbを送信し、これにより、ユーザホームネットワーク303のユーザが決済機関91に支払った金銭が、コンテンツプロバイダ301およびサービスプロバイダ310a, 310bの所有者に分配される。

上述したように、EMDシステム300bによれば、同じコンテンツファイル CFをサービスプロバイダに310a,310bに供給する場合に、当該コンテンツファイルCFについての権利書データ106を配信用鍵データKD1~KD で暗号化してサービスプロバイダに310a,310bに供給し、サービスプロバイダに310a,310bに供給し、サービスプロバイダに310a,310bに借利書データ106をそのまま格納したセキュアコンテナ304a,304bをユーザホームネットワークに配給する。そのため、ユーザホームネットワーク内のSAM3051~3054では、コンテンツファイルCFをサービスプロバイダに310a,310bの何れから配給を受けた場合でも、共通の権利書データ106に基づいて権利処理を行うことができる。

なお、上述した第1変形例では、2個のサービスプロバイダを用いた場合を例 示したが、本発明では、サービスプロバイダの数は任意である。

#### 第2実施形態の第2変形例

図81は、第2実施形態の第2変形例に係わる複数のコンテンツプロバイダを 用いたEMDシステム300bの構成図である。

図81において、図49と同一符号を付した構成要素は、第2実施形態で説明 した同一符号の構成要素と同じである。

図81に示すように、EMDシステム300bでは、コンテンツプロバイダ301a,301bからサービスプロバイダ310に、それぞれセキュアコンテナ104a,104bが供給される。

サービスプロバイダ310は、例えば、コンテンツプロバイダ301a, 301bが供給したコンテンツを用いてサービスを提供しており、セキュアコンテナ104aについてのプライスタグデータ312aと、セキュアコンテナ104bについてのプライスタグデータ312bとをそれぞれ生成し、これらを格納したセキュアコンテナ304cを作成する。

図81に示すように、セキュアコンテナ304 cには、コンテンツファイルC Fa, CFb、キーファイルKFa, KFb、プライスタグデータ312a, 312b、それらの各々についてのサービスプロバイダ310の秘密鍵データKcp sによる署名データが格納されている。

 $SAM3051 \sim 305$ 。では、配信用鍵データ $KDa1 \sim KDas$ を用いて、キーファイルKFaが復号され、権利書データ106aに基づいて、コンテンツファイルCFaについてのユーザからの操作に応じた購入・利用に関する処理が行われ、その履歴が利用履歴データ308に記述される。

また、SAM3051~3051において、配信用鍵データKDb1~KDb 。を用いて、キーファイルKFbが復号され、権利書データ106bに基づいて 、コンテンツファイルCFbについてのユーザからの操作に応じた購入・利用に

関する処理が行われ、その履歴が利用履歴データ308に記述される。

そして、 $SAM3051\sim305$  からEMDサービスセンタ302に、利用履歴データ308が送信される。

EMDサービスセンタ302では、利用履歴データ308に基づいて、コンテンツプロバイダ301a,301bおよびサービスプロバイダ310の各々について、課金内容を決定(計算)し、その結果に基づいて、それぞれに対応する決済請求権データ152ca,152cb,152sを作成する。

EMDサービスセンタ302は、ペイメントゲートウェイ90を介して決済機関91に、決済請求権データ152ca, 152cb, 152sを送信し、これにより、ユーザホームネットワーク303のユーザが決済機関91に支払った金銭が、コンテンツプロバイダ301a, 301bおよびサービスプロバイダ310の所有者に分配される。

上述したように、EMDシステム300bによれば、セキュアコンテナ304 c内に格納されたコンテンツファイルCFa, CFbの権利書デー9106a, 106bは、コンテンツプロバイダ301a, 301bが作成したものをそのまま用いるため、SAM3051  $\sim 305$ 4 内において、権利書デー9106a, 106bに基づいて、コンテンツファイルCFa, CFbについての権利処理がコンテンツプロバイダ301a, 301bの意向に沿って確実に行われる。

なお、図81に示す第2変形例では、2個のコンテンツプロバイダを用いた場合を例示したが、コンテンツプロバイダの数は任意である。

また、コンテンツプロバイダおよびサービスプロバイダの双方が複数であってもよい。

## 第2実施形態の第3変形例

図82は、第2実施形態の第3変形例に係わるEMDシステムの構成図である

上述した第2実施形態では、EMDサービスセンタ302が決済機関91に対

して、コンテンツプロバイダ301およびサービスプロバイダ310の決済を行う場合を例示したが、本発明では、例えば、図82に示すように、EMDサービスセンタ302において、利用履歴データ308に基づいて、コンテンツプロバイダ301のための決済請求権データ152cと、サービスプロバイダ310のための決済請求権データ152sとを作成し、これらをそれぞれコンテンツプロバイダ301およびサービスプロバイダ310に送信するようにしてもよい。

この場合には、コンテンツプロバイダ301は、決済請求権データ152cを用いて、ペイメントゲートウェイ90aを介して決済機関91aに決済を行う。また、サービスプロバイダ310は、決済請求権データ152sを用いて、ペイメントゲートウェイ90bを介して決済機関91bに決済を行う。

#### 第2実施形態の第4変形例

図83は、第2実施形態の第4変形例に係わるEMDシステムの構成図である

上述した第2実施形態では、例えば現行のインターネットのようにサービスプロバイダ310が課金機能を有していない場合を例示したが、現行のデジタル放送などのようにサービスプロバイダ310が課金機能を有している場合には、CAモジュール311において、セキュアコンテナ304に関するサービスプロバイダ310のサービスに対しての利用履歴データ308sを作成してサービスプロバイダ310に送信する。

そして、サービスプロバイダ310は、利用履歴データ308sに基づいて、 課金処理を行って決済請求権データ152sを作成し、これを用いてペイメント ゲートウェイ90bを介して決済機関91bに決済を行う。

一方、SAM3051~305。は、セキュアコンテナ304に関するコンテンツプロバイダ301の権利処理に対しての利用履歴データ308cを作成し、これをEMDサービスセンタ302に送信する。

EMDサービスセンタ302は、利用履歴データ308cに基づいて、決済請

求権データ152cを作成し、これをコンテンツプロバイダ301に送信する。 コンテンツプロバイダ301は、決済請求権データ152cを用いて、ペイメ ントゲートウェイ90aを介して決済機関91aに決済を行う。

#### 第2実施形態の第5変形例

上述した実施形態では、図49に示すように、EMDサービスセンタ302のユーザ嗜好フィルタ生成部901において、SAM3051などから受信した利用履歴データ308に基づいて、ユーザ嗜好フィルタデータ903を生成する場合を例示したが、例えば、図67に示すSAM3051などの利用監視部186で生成した利用制御状態データ166をリアルタイムでEMDサービスセンタ302に送信するようにして、SP用購入履歴データ309において、利用制御状態データ166に基づいてユーザ嗜好フィルタデータ903を生成するようにしてもよい。

### 第2実施形態の第6変形例

コンテンツプロバイダ301、サービスプロバイダ310およびSAM305  $1 \sim 3054$  は、それぞれ自らの公開鍵データ $K_{CP,P}$ ,  $K_{SP,P}$ ,  $K_{SAM1,P} \sim K_{SAM4,P}$ の他に、自らの秘密鍵データ $K_{CP,S}$ ,  $K_{SP,S}$ ,  $K_{SAM1,S} \sim K_{SAM4,S} \approx EMD$  サービスセンタ302に登録してもよい。

このようにすることで、EMDサービスセンタ302は、緊急時に、国家あるいは警察機関などからの要請に応じて、秘密鍵データ $K_{CP.S}$ ,  $K_{SP.S}$ ,  $K_{SAM1.S}$   $\sim K_{SAM4.S}$ を用いて、コンテンツプロバイダ301とサービスプロバイダ310 との間の通信、サービスプロバイダ310と $SAM3051\sim305$ 。 との間の通信、並びにユーザホームネットワーク303内での $SAM3051\sim305$ 。相互間での通信のうち対象となる通信を盗聴することが可能になる。

また、 $SAM3051 \sim 3054$  については、出荷時に、EMDサービスセンタ302によって秘密鍵データ $K_{SAM1.S} \sim K_{SAM4.S}$ を生成し、これを $SAM3051 \sim 3054$  に格納すると共にEMDサービスセンタ302が保持(登録)す

るようにしてもよい。

#### 第2実施形態の第7変形例

上述した実施形態では、コンテンツプロバイダ301、サービスプロバイダ310 およびSAM3051~3051が、相互に通信を行う場合に、EMDサービスセンタ302から事前に公開鍵証明書データ $CER_{CP}$ ,  $CER_{SP}$ ,  $CER_{SAN4}$  を取得し、イン・バンド方式で通信先に送信する場合を例示したが、本発明では、通信先への公開鍵証明書データの送信形態として種々の形態を採用できる。

例えば、コンテンツプロバイダ301、サービスプロバイダ310および $SAM3051\sim305$ 。が、相互に通信を行う場合に、EMDサービスセンタ302から事前に公開鍵証明書データCER<sub>CP</sub>、CER<sub>SP</sub>、CER<sub>SAM1</sub>~CER<sub>SAM2</sub>を取得し、当該通信に先立ってアウト・オブ・バンド方式で通信先に送信してもよい。

また、コンテンツプロバイダ301、サービスプロバイダ310およびSAM  $3051 \sim 3054$  が、通信時に、EMDサービスセンタ302から公開鍵証明 書データCER<sub>SP</sub>, CER<sub>SP</sub>, CER<sub>SAM1</sub>  $\sim$  CER<sub>SAM4</sub> を取得してもよい。

図84は、公開鍵証明書データの取得(入手)ルートの形態を説明するための図である。

なお、図84において、図49と同じ符号を付した構成要素は、前述した同一符号の構成要素と同じである。また、ユーザホームネットワーク303aは、前述したユーザホームネットワーク303と同じである。ユーザホームネットワーク303bでは、IEEE1394シリアルバスであるバス191を介してSAM30511~30514を接続している。

コンテンツプロバイダ301がサービスプロバイダ310の公開鍵証明書データCERspを取得する場合には、例えば、通信に先立ってサービスプロバイダ3 10からコンテンツプロバイダ301に公開鍵証明書データCERspを送信する

場合(図84中(3))と、コンテンツプロバイダ301がEMDサービスセンタ302から公開鍵証明書データCERspを取り寄せる場合(図84中(1))とがある。

また、サービスプロバイダ310がコンテンツプロバイダ301の公開鍵証明書データCERcrを取得する場合には、例えば、通信に先立ってコンテンツプロバイダ301からサービスプロバイダ310に公開鍵証明書データCERcrを送信する場合(図84中(2))と、サービスプロバイダ310がEMDサービスセンタ302から公開鍵証明書データCERcrを取り寄せる場合(図84中(4))とがある。

また、サービスプロバイダ310がSAM3051~305.の公開鍵証明書データCER<sub>SAM1</sub>~CER<sub>SAM4</sub>を取得する場合には、例えば、通信に先立ってSAM3051~305.からサービスプロバイダ310に公開鍵証明書データCER<sub>SAM1</sub>~CER<sub>SAM4</sub>を送信する場合(図84中(6))と、サービスプロバイダ310がEMDサービスセンタ302から公開鍵証明書データCER<sub>SAM1</sub>~CER<sub>SAM4</sub>を取り寄せる場合(図84中(4))とがある。

また、SAM3051 ~305  $\iota$  がサービスプロバイダ310の公開鍵証明書データCERspを取得する場合には、例えば、通信に先立ってサービスプロバイダ310からSAM3051 ~305  $\iota$  に公開鍵証明書データCERspを送信する場合(図84中(5))と、SAM3051 ~305  $\iota$  がEMD サービスセンタ302から公開鍵証明書データCERspを取り寄せる場合(図84中(7)など)とがある。

また、SAM3051がSAM3052の公開鍵証明書データCERsam2を取得する場合には、例えば、通信に先立ってSAM3052からSAM3051に公開鍵証明書データCERsam2を送信する場合(図84中(8))と、SAM3051がEMDサービスセンタ302から公開鍵証明書データCERsam2を取り寄せる場合(図84中(7)など)とがある。

また、SAM3052がSAM3051の公開鍵証明書データCERsam1を取得する場合には、例えば、通信に先立ってSAM3051からSAM3052に公開鍵証明書データCERsam1を送信する場合(図84中(9))と、SAM3052が自らEMDサービスセンタ302から公開鍵証明書データCERsam1を取り寄せる場合と、SAM3051が搭載されたネットワーク機器を介して公開鍵証明書データCERsam1を取り寄せる場合(図84中(7),(8))とがある。

また、SAM305』がSAM3051sの公開鍵証明書データCERsam1s を取得する場合には、例えば、通信に先立ってSAM3051sからSAM3051 に公開鍵証明書データCERsam1s を送信する場合(図84中(12))と、SAM3051が自らEMDサービスセンタ302から公開鍵証明書データCERsam1s を取り寄せる場合(図84中(10))と、ユーザホームネットワーク303b内のネットワーク機器を介して公開鍵証明書データCERsam1s を取り寄せる場合とがある。

また、SAM3051sがSAM3054の公開鍵証明書データCERsam4を取得する場合には、例えば、通信に先立ってSAM3054からSAM3051sに公開鍵証明書データCERsam4を送信する場合(図84中(11))と、SAM3051sが自らEMDサービスセンタ302から公開鍵証明書データCERsam4を取り寄せる場合(図84中(13))と、ユーザホームネットワーク303b内のネットワーク機器を介して公開鍵証明書データCERsam4を取り寄せる場合とがある。

第2実施形態における公開鍵証明書破棄リスト(データ)の取り扱い

第2実施形態では、EMDサービスセンタ302において、不正行為などに用いられたコンテンツプロバイダ301、サービスプロバイダ310およびSAM305 $_1$ ~305 $_4$ が他の装置と通信できないようにするために、当該不正行為に用いられた装置の公開鍵証明書データを無効にする公開鍵証明書破棄データを

作成する。そして、当該公開鍵証明書破棄データCRL(Certificate Revocation List)を、コンテンツプロバイダ301、サービスプロバイダ310および $SAM3051\sim305$ 。に送信する。

なお、公開鍵証明書破棄データCRLは、EMDサービスセンタ302の他に、例えば、コンテンツプロバイダ301、サービスプロバイダ310およびSAM3051  $\sim 305$ 4 において生成してもよい。

先ず、EMDサービスセンタ302が、コンテンツプロバイダ301の公開鍵証明書データCERcrを無効にする場合について説明する。

図85に示すように、EMDサービスセンタ302は、公開鍵証明書データCERcrを無効にすることを示す公開鍵証明書破棄データCRL1をサービスプロバイダ310に送信する(図85中(1))。サービスプロバイダ310は、コンテンツプロバイダ301から入力した署名データを検証する際に、公開鍵証明書破棄データCRL1を参照して公開鍵証明書データCERcrの有効性を判断し、有効であると判断した場合に公開鍵データKcrrrを用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずにコンテンツプロバイダ301からのデータを無効にする。なお、データを無効にするのではなく、通信を拒絶するようにしてもよい。

また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL1を、サービスプロバイダ310の流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク303内の例えばSAM3051に送信する(図85中(1),(2))。SAM3051は、サービスプロバイダ310から入力したセキュアコンテナ内に格納されたコンテンツプロバイダ301の署名データを検証する際に、公開鍵証明書破棄データCRL1を参照して公開鍵証明書データCERcpの有効性を判断し、有効であると判断した場合に公開鍵データ $K_{CP,P}$ を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該セキュアコンテナを無効にする。

なお、EMDサービスセンタ302は、公開鍵証明書破棄データCRL1を、 ユーザホームネットワーク303内のネットワーク機器を介してSAM3051 に直接送信してもよい(図85中(3))。

次に、EMDサービスセンタ302が、サービスプロバイダ310の公開鍵証明書データCERsrを無効にする場合について説明する。

図86に示すように、EMDサービスセンタ302は、公開鍵証明書データCERspを無効にすることを示す公開鍵証明書破棄データCRL2をコンテンツプロバイダ301に送信する(図86中(1))。コンテンツプロバイダ301は、サービスプロバイダ310から入力した署名データを検証する際に、公開鍵証明書破棄データCRL2を参照して公開鍵証明書データCERspの有効性を判断し、有効であると判断した場合に公開鍵データKsp.pe用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずにサービスプロバイダ310からのデータを無効にする。

また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL2を、サービスプロバイダ310の流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク303内の例えばSAM3051に送信する(図86中(2))。SAM3051は、サービスプロバイダ310から入力したセキュアコンテナ内に格納されたサービスプロバイダ310の署名データを検証する際に、公開鍵証明書破棄データCRL2を参照して公開鍵証明書データCERspの有効性を判断し、有効であると判断した場合に公開鍵デーKsp.pを用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該セキュアコンテナを無効にする。

この場合に、サービスプロバイダ310内において、公開鍵証明書破棄データ CRL2の送受信を行うモジュールは、耐タンパ性を有している必要がある。また、サービスプロバイダ310内において、公開鍵証明書破棄データCRL2は、サービスプロバイダ310の関係者による改竄な困難な領域に格納される必要

がある。

なお、EMDサービスセンタ302は、公開鍵証明書破棄データCRL2を、 ユーザホームネットワーク303内のネットワーク機器を介してSAM3051 に直接送信してもよい(図86中(3))。

次に、EMDサービスセンタ302が、例えばSAM3052の公開鍵証明書 データCERsam2を無効にする場合について説明する。

図87に示すように、EMDサービスセンタ302は、公開鍵証明書データCERsam2を無効にすることを示す公開鍵証明書破棄データCRLsをコンテンツプロバイダ301に送信する(図87中(1))。コンテンツプロバイダ301は、公開鍵証明書破棄データCRLsをサービスプロバイダ310に送信する。サービスプロバイダ310は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク303内の例えばSAM3051に公開鍵証明書破棄データCRLsam1を送信する(図87中(1))。SAM3051は、SAM3052から入力したデータに付加されたSAM3052の署名データを検証する際に、公開鍵証明書破棄データCRLsを参照して公開鍵証明書データCERsam2の有効性を判断し、有効であると判断した場合に公開鍵データKsam2 Pを用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該データを無効にする。

この場合に、サービスプロバイダ310内において、公開鍵証明書破棄データ CRLs の送受信を行うモジュールは、耐タンパ性を有している必要がある。また、サービスプロバイダ310内において、公開鍵証明書破棄データCRLs は、サービスプロバイダ310の関係者による改竄な困難な領域に格納される必要 がある。

EMDサービスセンタ302は、公開鍵証明書破棄データCRLsをサービスプロバイダ310を介してSAM3051に送信してもよい(図87中(1),(2))。

また、EMDサービスセンタ302は、公開鍵証明書破棄データ $CRL_s$ を、ユーザホームネットワーク303内のネットワーク機器を介して $SAM305_1$ に直接送信してもよい(図87中(3))。

また、EMDサービスセンタ302は、例えばSAM3052の公開鍵証明書データ $CER_{SAM2}$ を無効にすることを示す公開鍵証明書破棄データ $CRL_8$ を作成し、これを保管する。

また、ユーザホームネットワーク303は、バス191に接続されているSAMのSAM登録リストSRLを作成し、これをEMDサービスセンタ302に送信する(図88中(1))。

EMDサービスセンタ302は、SAM登録リストに示されるSAM3051~3054のうち、公開鍵証明書破棄データCRL8によって無効にすることが示されているSAM(例えばSAM3052)を特定し、SAM登録リストSR L内の当該SAMに対応する破棄フラグを無効を示すように設定して新たなSAM 登録リストSRLを作成する。

次に、EMDサービスセンタ302は、当該生成したSAM登録リストSRL をSAM3051に送信する(図88中(1))。

SAM3051は、他のSAMと通信を行う際に、SAM登録リストSRLの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

また、EMDサービスセンタ302は、公開鍵証明書破棄データCRLsを作成し、これをコンテンツプロバイダ301に送信する(図88中(2))。

コンテンツプロバイダ301は、公開鍵証明書破棄データCRL。をサービスプロバイダ310に送信する(図88中(2))。

次に、サービスプロバイダ310は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、公開鍵証明書破棄データCRLsをSAM3051に送信する(図88中(2))。

SAM3051 は、自らが作成したSAM登録リストに示されるSAM3051 ~ 3054 のうち、公開鍵証明書破棄データCRL8 によって無効にすることが示されているSAM (例えばSAM3052 )を特定し、SAM登録リストSRL内の当該SAMに対応する破棄フラグを無効を示すように設定する。

以後、SAM3051は、他のSAMと通信を行う際に、当該SAM登録リストSRLの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

また、EMDサービスセンタ302は、公開鍵証明書破棄データCRLsを作成し、これをサービスプロバイダ310に送信する(図88中(3))。

次に、サービスプロバイダ310は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、公開鍵証明書破棄データCRL®をSAM3051に送信する(図88中(3))。

SAM3051は、自らが作成したSAM登録リストに示されるSAM305 $_1\sim305$ 4のうち、公開鍵証明書破棄データCRL $_2$ 8によって無効にすることが示されているSAM(例えばSAM305 $_2$ )を特定し、SAM登録リストSRL内の当該SAMに対応する破棄フラグを無効を示すように設定する。

以後、SAM3051は、他のSAMと通信を行う際に、当該SAM登録リストSRLの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

# EMDサービスセンタ302の役割等

図89は、図49に示すEMDサービスセンタ(クリアリングハウス))302の機能を権利管理用クリアリングハウス950と、電子決済用クリアリングハウス951とに分割した場合のEMDシステムの構成図である。

当該EMDシステムでは、電子決済用クリアリングハウス 9 5 1 において、ユーザホームネットワーク 3 0 3 a, 3 0 3 bのSAMからの利用履歴データ 3 0 8 に基づいて、決済処理(利益分配処理)を行い、コンテンツプロバイダ 3 0 1

およびサービスプロバイダ3 1 0 の決済請求権データをそれぞれ生成し、ペイメントゲートウェイ 9 0 を介して決済機関 9 1 において決済を行う。

また、権利管理用クリアリングハウス 9 5 0 は、電子決済用クリアリングハウス 9 5 1 からの決済通知に応じたコンテンツプロバイダ 3 0 1 およびサービスプロバイダ 3 1 0 の決済レポートを作成し、それらをコンテンツプロバイダ 3 0 1 およびコンテンツプロバイダ 3 0 1 に送信する。

また、コンテンツプロバイダ301の権利書データ106およびコンテンツ鍵 データKcの登録(権威化)などを行う。

なお、図90に示すように、権利管理用クリアリングハウス950と電子決済 用クリアリングハウス951とを単体の装置内に収納すると、図49に示すEM Dサービスセンタ302となる。

また、本発明は、例えば、図91に示すように、EMDサービスセンタ302に、権利管理用クリアリングハウス960の機能を設け、権利管理用クリアリングハウス960において、権利書データ106の登録などを行うと共に、SAMからの利用履歴データ308に基づいてサービスプロバイダ310の決済請求権データを作成し、これをサービスプロバイダ310に送信してもよい。この場合には、サービスプロバイダ310は、自らの課金システムを電子決済用クリアリングハウス961として利用し、権利管理用クリアリングハウス960からの決済請求権データに基づいて決済を行う。

また、本発明は、例えば、図92に示すように、EMDサービスセンタ302に、権利管理用クリアリングハウス970の機能を設け、権利管理用クリアリングハウス970において、権利書データ106の登録などを行うと共に、SAMからの利用履歴データ308に基づいてコンテンツプロバイダ301の決済請求権データを作成し、これをコンテンツプロバイダ301に送信してもよい。この場合には、コンテンツプロバイダ301は、自らの課金システムを電子決済用クリアリングハウス961として利用し、権利管理用クリアリングハウス970か

らの決済請求権データに基づいて決済を行う。

#### 第2実施形態の第8変形例

上述した第2実施形態では、図49に示すEMDシステム300において、コンテンツプロバイダ301からサービスプロバイダ310に図4に示すフォーマットのセキュアコンテナ104を提供し、サービスプロバイダ310からユーザホームネットワーク303に図53に示すフォーマットのセキュアコンテナ304を配給する場合を例示した。

すなわち、上述した第2実施形態では、図4および図53に示すように、セキュアコンテナ104およびセキュアコンテナ304内に、それぞれ単数のコンテンツファイルCFと、当該コンテンツファイルCFに対応する単数のキーファイルKFを格納した場合を例示した。

本発明では、セキュアコンテナ104およびセキュアコンテナ304内に、それぞれ複数のコンテンツファイルCFと、当該複数のコンテンツファイルCFに それぞれ対応する複数のキーファイルKFとを格納してもよい。

図93は、本変形例において、図49に示すコンテンツプロバイダ301から サービスプロバイダ310に提供されるセキュアコンテナ104aのフォーマットを説明するための図である。

ここで、署名データSI $G_{250, CP}$ は、コンテンツプロバイダ301において、コンテンツファイル $CF_{101}$ ,  $CF_{102}$ ,  $CF_{108}$  、キーファイル $KF_{101}$ ,  $KF_{102}$ ,  $KF_{108}$  、公開鍵証明書データ $CER_{CP}$ および署名データ $SIG_{1.BSC}$ の全体に対してハッシュ値をとり、コンテンツプロバイダ301の秘密鍵データ  $K_{CP,S}$ を用いて生成される。

コンテンツファイル $CF_{101}$  には、ヘッダ、リンクデータ $LD_1$ 、メタデータ $Meta_1$ 、コンテンツデータ $C_1$  およびA/V伸長用ソフトウェア $Soft_1$  が格納されている。

ここで、コンテンツデータ $C_1$  およびA/V伸長用ソフトウェア $Soft_1$  は、前述したコンテンツ鍵データ $Kc_1$  を用いて暗号化されており、メタデータM etal は必要に応じてコンテンツ鍵データ $Kc_1$  を用いて暗号化されている。

また、コンテンツデータ $C_1$  は、例えば、ATRAC 3 方式で圧縮されている。A/V伸長用ソフトウェア $S_0$  f  $t_1$  は、ATRAC 3 方式の伸長用のソフトウェアである。

また、リンクデータ $LD_1$  は、キーファイル $KF_{101}$  にリンクすることを示している。

コンテンツファイル $CF_{102}$  には、ヘッダ、リンクデータ $LD_1$  、メタデータ $Meta_2$  、コンテンツデータ $C_2$  およびA/V伸長用ソフトウェア $Soft_2$  が格納されている。

ここで、コンテンツデータ $C_2$  およびA/V伸長用ソフトウェア $Soft_2$  は、前述したコンテンツ鍵データ $Kc_2$  を用いて暗号化されており、メタデータMeta2 は必要に応じてコンテンツ鍵データ $Kc_2$  を用いて暗号化されている。

また、コンテンツデータ $C_2$  は、例えば、MPEG 2 方式で圧縮されている。 A / V伸長用ソフトウェア $S_0$  f  $t_2$  は、MPEG 2 方式の伸長用のソフトウェアである。

、また、リンクデータ $LD_2$  は、キーファイル $KF_{102}$  にリンクすることを示している。

コンテンツファイル $CF_{108}$  には、ヘッダ、リンクデータ $LD_8$  、メタデータ $Meta_8$  、コンテンツデータ $C_8$  およびA/V伸長用ソフトウェア $Soft_8$  が格納されている。

ここで、コンテンツデータCsおよびA/V伸長用ソフトウェアSoftsは

、前述したコンテンツ鍵データKcsを用いて暗号化されており、メタデータMetasは必要に応じてコンテンツ鍵データKcsを用いて暗号化されている。

また、コンテンツデータ $C_s$  は、例えば、JPEG方式で圧縮されている。A / V伸長用ソフトウェア $S_0$  f t s は、JPEG方式の伸長用のソフトウェアである。

また、リンクデータ $LD_s$  は、キーファイル $KF_{10s}$  にリンクすることを示している。

キーファイル $KF_{101}$  には、ヘッダと、それぞれ配信鍵データ $KD_1 \sim KD_8$  を用いて暗号化されたコンテンツ鍵データ $Kc_1$ 、権利書データ $106_1$ 、SA  $Mプログラム・ダウンロード・コンテナSDC_1 および署名・証明書モジュール <math>Mod_{200}$  とが格納されている。

ここで、署名・証明書モジュール $Mod_{200}$  には、図94Aに示すように、それぞれコンテンツデータ $C_1$  , コンテンツ鍵データ $Kc_1$  および権利書データ $106_1$  のハッシュ値をとり、コンテンツプロバイダ301の秘密鍵データ $Kc_P$  、 sを用いて作成した署名データ $SIG_{211, CP}$  、 $SIG_{212, CP}$  、 $SIG_{218, CP}$  と、公開鍵データ $K_{CP, P}$ の公開鍵証明書データ $CER_{CP}$  と、当該公開鍵証明書データ $CER_{CP}$  と対してのEMD サービスセンタ302 の署名データ $SIG_{1, BSC}$  とが格納されている。

キーファイル $KF_{102}$  には、ヘッダと、それぞれ配信鍵データ $KD_1 \sim KD_3$  を用いて暗号化されたコンテンツ鍵データ $Kc_2$  、権利書データ $106_2$  、SA  $Mプログラム・ダウンロード・コンテナ<math>SDC_2$  および署名・証明書モジュール  $Mod_{201}$  とが格納されている。

ここで、署名・証明書モジュール $Mod_{201}$  には、図94Bに示すように、それぞれコンテンツデータ $C_2$  , コンテンツ鍵データ $Kc_2$  および権利書データ $106_2$  のハッシュ値をとり、コンテンツプロバイダ301の秘密鍵データ $Kc_{P.}$  sを用いて作成した署名データ $SIG_{221,CP}$ ,  $SIG_{222,CP}$ ,  $SIG_{223,CP}$ 

開鍵証明書データCERcrと、当該公開鍵証明書データCERcrに対しての署名データSIG1. BSc とが格納されている。

キーファイルKF10s には、ヘッダと、それぞれ配信鍵データKD1 ~KDs を用いて暗号化されたコンテンツ鍵データKcs、権利書データ106s、SA Mプログラム・ダウンロード・コンテナSDCs および署名・証明書モジュール Mod20s とが格納されている。

ここで、署名・証明書モジュール $Mod_{202}$  には、図94Cに示すように、それぞれコンテンツデータCs , コンテンツ鍵データKcs および権利書データ106s のハッシュ値をとり、コンテンツプロバイダ301の秘密鍵データKcr , sを用いて作成した署名データ $SIG_{281, cr}$  ,  $SIG_{282, cr}$  ,  $SIG_{288, cr}$  と、公開鍵証明書データ $CER_{cr}$ と、当該公開鍵証明書データ $CER_{cr}$ に対しての署名データ $SIG_{1, BSC}$  とが格納されている。

サービスプロバイダ310は、図93に示すセキュアコンテナ104 $\alpha$ の配給を受けると、EMDサービスセンタ302の公開鍵データ $K_{BSC,P}$ を用いて公開鍵証明書データ $CER_{cP}$ の正当性を確認した後に、当該公開鍵証明書データ $CER_{cP}$ に格納された公開鍵データ $K_{cP,P}$ を用いて、署名データ $SIG_{250,CP}$ の正当性を確認する。

そして、サービスプロバイダ310は、署名データSIG250.cpの正当性を確認すると、図95に示すように、セキュアコンテナ104aから得たコンテンツファイルCF101, CF102, CF10s およびキーファイルKF101, KF102, KF10s と、サービスプロバイダ310の公開鍵証明書データCERspと、署名データSIG81.BSCと、プライスタグデータ3121, 3122, 312s と、署名データSIG280.spとを格納したセキュアコンテナ304aを作成する。ここで、プライスタグデータ3121, 3122, 312s は、それぞれコンテンツデータC1, C2, C3の販売価格を示している。

また、署名データSIG280, spは、コンテンツファイルCF101, CF102,

 $CF_{108}$ 、キーファイル $KF_{101}$ ,  $KF_{102}$ ,  $KF_{108}$ 、公開鍵証明書データ $CER_{SP}$ と、署名データ $SIG_{81,8SC}$ およびプライスタグデータ $312_1$ ,  $312_2$ ,  $312_3$  の全体に対してハッシュ値をとり、サービスプロバイダ310の秘密鍵データ $K_{SP,S}$ を用いて生成される。

サービスプロバイダ310は、図95に示すセキュアコンテナ304aをユーザホームネットワーク303に配給する。

ューザホームネットワーク303では、 $SAM3051\sim3054$  において、セキュアコンテナ304 a に格納された署名データ $SIG_{81, BSC}$ の正当性を確認した後に、公開鍵証明書データ $CER_{sp}$ に格納された公開鍵データ $K_{SP, KP}$  を用いて、署名データ $SIG_{280, SP}$ の正当性を確認する。

その後、 $SAM3051 \sim 305 \iota$  は、コンテンツデータ $C_{101}$  ,  $C_{102}$  ,  $C_{103}$  についての権利処理を、リンクデータ $LD_1$  ,  $LD_2$  ,  $LD_3$  に示されるリンク状態に応じて、それぞれキーファイル $KF_{101}$  ,  $KF_{102}$  ,  $KF_{103}$  に基づいて行う。

なお、上述した第8変形例では、コンテンツプロバイダ301において、図93に示すように、コンテンツプロバイダ301において、コンテンツファイルCF101, CF102, CF103、キーファイルKF101, KF102, KF103、公開鍵証明書データCERcpおよび署名データSIG1. BSC の全体に対しての署名データSIG250. Cpを作成する場合を例示したが、例えば、コンテンツファイルCF101, CF102, CF103 およびキーファイルKF101, KF102, KF103のそれぞれについて署名データを作成し、これをセキュアコンテナ104a内に格納してもよい。

また、上述した第8変形例では、サービスプロバイダ310において、図95に示すように、コンテンツファイルCF101, CF102, CF103、キーファイルKF101, KF102, KF108、公開鍵証明書データCERspと、署名データSIG61, BSCおよびプライスタグデータ3121, 3122, 3128 の全体に

対しての署名データSIG280、spを作成する場合を例示したが、これらの各々についての署名データを作成し、これらをセキュアコンテナ304aに格納するようにしてもよい。

また、上述した第8変形例では、セキュアコンテナ304において、単数のサービスプロバイダ310から提供を受けた複数のコンテンツファイルCF101, CF102, CF108 を単数のセキュアコンテナ304aに格納してユーザホームネットワーク303に配給する場合を例示したが、図81に示すように、複数のコンテンツプロバイダ301a, 301bから提供を受けた複数のコンテンツファイルCFを、単数のセキュアコンテナに格納してユーザホームネットワーク303に配給してもよい。

なお、図93に示すフォーマットは、前述した第1実施形態において、図1に 示すコンテンツプロバイダ101からユーザホームネットワーク103にセキュ アコンテナ104を送信する場合にも同様に適用できる。

また、上述した実施形態では、EMDサービスセンタにおいて、SAMから入力した利用履歴データに基づいて決済処理を行う場合を例示したが、SAMにおいてコンテンツの購入形態が決定される度に利用制御状態データをSAMからEMDサービスセンタに送信し、EMDサービスセンタにおいて、受信した利用制御状態データを用いて決済処理を行ってもよい。

以下、コンテンツプロバイダ101において作成されるコンテンツファイルC FおよびキーファイルKFなどの概念をまとめる。

コンテンツプロバイダ101がインターネットを用いてコンテンツを提供する場合には、図96に示すように、ヘッダ、コンテンツID、コンテンツ鍵データ Kcを用いた暗号化されたコンテンツデータCおよび署名データを含むコンテンツファイルCFが作成される。当該コンテンツデータCの取り扱いを示す権利書データと、コンテンツ鍵データKcとが、所定の信頼機関であるEMDサービスセンタ102, 302の配信用鍵データによって暗号化された後に、キーファイ

ルKFに格納される。また、キーファイルKFには、ヘッダ、コンテンツID、 必要に応じてメタデータ、署名データが格納される。

そして、コンテンツファイルCFおよびキーファイルKFが、コンテンツプロバイダ101からユーザホームネットワーク103,303に直接提供されたり、コンテンツプロバイダ101からサービスプロバイダ310を介してユーザホームネットワーク103,303に提供される。

また、コンテンツプロバイダ101がインターネットを用いてコンテンツを提供する場合に、図97に示すように、キーファイルKF内にコンテンツ鍵データ K c を格納しないで、所定の信頼機関であるEMDサービスセンタ102,302の配信用鍵データによって暗号化したコンテンツ鍵データK c をEMDサービスセンタ102,302からユーザホームネットワーク103,303に提供してもよい。

また、コンテンツプロバイダ101がデジタル放送を用いてコンテンツを提供する場合に、例えば、図98に示すように、コンテンツ鍵データKcを用いて暗号化したコンテンツデータCと署名データとを、コンテンツプロバイダ101からユーザホームネットワーク103,303に、直接あるいはサービスプロバイダ310を介して提供する。この場合に、図97に示すキーファイルKFに対応する鍵データブロックを、コンテンツプロバイダ101からユーザホームネットワーク103,303に、直接あるいはサービスプロバイダ310を介して提供する。

また、この場合に、例えば、図99に示すように、所定の信頼機関であるEMDサービスセンタ102,302の配信用鍵データによって暗号化したコンテンツ鍵データK c をE MDサービスセンタ102,302からユーザホームネットワーク103,303に提供してもよい。

#### 産業上の利用可能性

以上説明したように、本発明によれば、データ提供装置の関係者の利益が適切 に保護される。

また、本発明によれば、権利書データなどが不正に改竄されることを適切に回 避できる。

また、本発明によれば、データ提供装置の関係者の利益を保護するための監査の負担を軽減できる。

#### 請求の範囲

1. データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された 前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書 データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

2. 前記データ提供装置は、配信用鍵データを用いてそれぞれ暗号化された 前記コンテンツ鍵データおよび前記権利書データを格納した前記モジュールを前 記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された 前記コンテンツ鍵データおよび前記権利書データを前記配信用鍵データを用いて 復号する

請求項1に記載のデータ提供システム。

3. 前記配信用鍵データを管理し、前記データ提供装置および前記データ処理装置に前記配信用鍵データを配給する管理装置

をさらに有する請求項2に記載のデータ提供システム。

4. 前記データ提供装置は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つに対して自らの署名データを作成し、当該作成した署名データを格納した前記モジュールを前記データ処理装置に配

#### 給する

請求項1に記載のデータ提供システム。

5. 前記データ提供装置は、自らの秘密鍵データを用いて前記署名データを 作成し、当該秘密鍵データに対応する公開鍵データを格納した前記モジュールを 前記データ処理装置に配給する

請求項4に記載のデータ提供システム。

6. 前記公開鍵データの正当性を証明する公開鍵証明書データを作成する管理装置

をさらに有し、

前記データ提供装置は、前記公開鍵証明書データを格納した前記モジュールを前記データ処理装置に配給する

請求項5に記載のデータ提供システム。

7. 前記データ提供装置は、

前記コンテンツデータを格納した第1のファイルと、

前記コンテンツ鍵データおよび前記権利書データを格納した第2のファイルとを格納した前記モジュールを前記データ処理装置に配給する

請求項1に記載のデータ提供システム。

8. 前記データ提供装置は、前記第1のファイルおよび前記第2のファイル について、自らの秘密鍵データを用いた署名データをそれぞれ作成し、当該作成 した署名データを格納した前記モジュールを前記データ処理装置に配給する

請求項7に記載のデータ提供システム。

9. 前記データ提供装置は、前記秘密鍵データに対応する公開鍵データを格 納した前記モジュールを前記データ処理装置に配給する

請求項8に記載のデータ提供システム。

10. 前記データ提供装置は、前記データ処理装置との間で相互認証を行い、 当該相互認証によって得たセッション鍵データを用いて前記モジュールを暗号化

し、当該暗号化したモジュールを前記データ処理装置に送信する 請求項1に記載のデータ提供システム。

- 11. 前記データ提供装置は、前記モジュールを記録した記録媒体を作成する 請求項1に記載のデータ提供システム。
- 12. 前記データ処理装置は、前記権利書データに基づいて、前記コンテンツ データの購入形態および利用形態の少なくとも一方を決定する

請求項1に記載のデータ提供システム。

13. 前記データ処理装置は、前記復号したコンテンツ鍵データと、前記暗号 化されたコンテンツデータとを復号装置に出力する

請求項1に記載のデータ提供システム。

14. 前記データ処理装置は、前記モジュールに格納された公開鍵データを用いて、前記モジュールに格納された署名データの正当性を検証する

請求項9に記載のデータ提供システム。

15. 前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理 装置における前記コンテンツデータの前記購入および前記利用に伴って得られた 利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う

請求項3に記載のデータ提供システム。

16. 前記データ処理装置は、その処理内容、内部メモリに記憶された所定のデータおよび処理中のデータを、外部から監視および改竄困難なモジュールからなる

請求項1に記載のデータ提供システム。

17. データ提供装置から配給されたコンテンツデータを利用するデータ処理

装置において、

コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号 化された権利書データとを格納したモジュールを前記データ提供装置から受けて、当該受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権 利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ処理装置。

18. データ提供装置、データ配給装置およびデータ処理装置を有するデータ 提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納 された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した 権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

19. 前記データ配給装置は、前記コンテンツデータの価格を示す価格データを格納した前記第2のモジュールを前記データ処理装置に配給する

請求項18に記載のデータ提供システム。

20. 前記データ提供装置は、配信用鍵データを用いてそれぞれ暗号化された前記コンテンツ鍵データおよび前記権利書データを格納した前記第1のモジュー

ルを前記データ配給装置に提供し、

前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを前記配信用鍵データを 用いて復号する

請求項18に記載のデータ提供システム。

21. 前記配信用鍵データを管理し、前記データ提供装置および前記データ処理装置に前記配信用鍵データを配給する管理装置

をさらに有する請求項20に記載のデータ提供システム。

22. 前記データ提供装置は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つに対して自らの署名データを作成し、当該作成した署名データを格納し、前記配信用鍵データを用いて暗号化された第3のモジュールを格納した前記第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記第3のモジュールを前記 第2のモジュールに格納して前記データ処理装置に配給する

請求項20に記載のデータ提供システム。

23. 前記データ提供装置は、自らの秘密鍵データを用いて前記署名データを 作成し、当該秘密鍵データに対応する公開鍵データを格納した前記第3のモジュ ールを格納した前記第1のモジュールを前記データ配給装置に提供する

請求項22に記載のデータ提供システム。

24. 前記公開鍵データの正当性を証明する公開鍵証明書データを作成する管理装置

をさらに有し、

前記データ提供装置は、前記公開鍵証明書データを格納した前記第3の モジュールを格納した前記第1のモジュールを前記データ配給装置に提供する 請求項23に記載のデータ提供システム。

25. 前記データ提供装置は、

前記コンテンツデータを格納した第1のファイルと、

前記コンテンツ鍵データおよび前記権利書データを格納した第2のファイルとを格納した前記第1のモジュールを前記データ配給装置に提供する

請求項18に記載のデータ提供システム。

26. 前記データ提供装置は、前記第1のファイルおよび前記第2のファイル について、自らの秘密鍵データを用いた署名データをそれぞれ作成し、当該作成 した署名データを格納した前記第1のモジュールを前記データ配給装置に提供す る

請求項25に記載のデータ提供システム。

27. 前記データ提供装置は、前記秘密鍵データに対応する公開鍵データを格 納した前記第1のモジュールを前記データ配給装置に提供する

請求項25に記載のデータ提供システム。

28. 前記データ配給装置は、前記価格データに対して自らの秘密鍵データを 用いて署名データを作成し、当該署名データを前記第2のモジュールに格納して 前記データ処理装置に配給する

請求項18に記載のデータ提供システム。

29. 前記データ提供装置は、前記自らの秘密鍵データに対応する公開鍵データを格納した前記第2のモジュールを前記データ処理装置に提供する

請求項28に記載のデータ提供システム。

- 30. 前記データ配給装置は、前記第1のファイルおよび前記第2のファイル についての署名データを、前記データ提供装置の公開鍵データを用いて検証する 請求項26に記載のデータ提供システム。
  - 31. 前記データ提供装置は、

前記第1のファイルと、第2のファイルとのリンク関係を示すリンクデータを格納した前記第1のモジュールを前記データ配給装置に提供する

請求項25に記載のデータ提供システム。

32. 前記データ配給装置は、前記データ処理装置との間で相互認証を行い、 当該相互認証によって得たセッション鍵データを用いて前記第2のモジュールを 暗号化し、当該暗号化した第2のモジュールを前記データ処理装置に送信する 請求項18に記載のデータ提供システム。

33. 前記データ配給装置は、前記モジュールを記録した記録媒体を作成する 請求項18に記載のデータ提供システム。

34. 前記データ処理装置は、前記権利書データに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する

請求項18に記載のデータ提供システム。

35. 前記データ処理装置は、前記復号したコンテンツ鍵データと、前記暗号 化されたコンテンツデータとを復号装置に出力する

請求項18に記載のデータ提供システム。

- 36. 前記データ処理装置は、前記第2のモジュールに格納された公開鍵データを用いて、前記第2のモジュールに格納された署名データの正当性を検証する 請求項29に記載のデータ提供システム。
- 37. 前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理 装置における前記コンテンツデータの前記購入および前記利用に伴って得られた 利益を、前記データ提供装置および前記データ配給装置の関係者に分配するため の利益分配処理を行う

請求項21に記載のデータ提供システム。

3.8. 前記データ処理装置は、その処理内容、内部メモリに記憶された所定の

データおよび処理中のデータを、外部から監視および**改竄**困難なモジュールからなる

請求項18に記載のデータ提供システム。

39. データ提供装置と、少なくとも第1のデータ配給装置および第2のデータ配給装置と、データ処理装置とを有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記複数のデータ配給装置に提供し、

前記第1のデータ配給装置は、前記提供を受けた前記第1のモジュール に格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権 利書データを格納した第2のモジュールを前記データ処理装置に配給し、

前記第2のデータ配給装置は、前記提供を受けた前記第1のモジュール に格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権 利書データを格納した第3のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第2のモジュールおよび 前記第3のモジュールに格納された前記コンテンツ鍵データおよび前記権利書デ ータを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの 取り扱いを決定する

データ提供システム。

40.少なくとも第1のデータ提供装置および第2のデータ提供装置と、データ配給装置と、データ処理装置とを有するデータ提供システムにおいて、

前記第1のデータ提供装置は、第1のコンテンツ鍵データを用いて暗号化された第1のコンテンツデータと、暗号化された前記第1のコンテンツ鍵データと、前記第1のコンテンツデータの取り扱いを示す暗号化された第1の権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、

前記第2のデータ提供装置は、第2のコンテンツ鍵データを用いて暗号 化された第2のコンテンツデータと、暗号化された前記第2のコンテンツ鍵デー タと、前記第2のコンテンツデータの取り扱いを示す暗号化された第2の権利書 データとを格納した第2のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化された前記第1のコンテンツデータ、前記第1のコンテンツ鍵データおよび前記第1の権利書データと、前記提供を受けた前記第2のモジュールに格納された前記暗号化された前記第2のコンテンツデータ、前記第2のコンテンツ鍵データおよび前記第2の権利書データとを格納した第3のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第3のモジュールに格納された前記第1のコンテンツ鍵データおよび前記第1の権利書データを復号し、当該復号した第1の権利書データに基づいて、前記第1のコンテンツデータの取り扱いを決定し、前記配給を受けた前記第3のモジュールに格納された前記第2のコンテンツ鍵データおよび前記第2の権利書データを復号し、当該復号した第2の権利書データに基づいて、前記第2のコンテンツデータの取り扱いを決定する

データ提供システム。

41. コンテンツデータの利用を行うデータ処理装置に、前記コンテンツデータを配給するデータ提供装置において、

コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号 化された権利書データとを格納したモジュールを前記データ処理装置に配給する

データ提供装置。

42. 前記権利書データを作成、当該作成した権利書データを格納した前記モジュールを前記データ処理装置に配給する

請求項41に記載のデータ提供装置。

43. 配信用鍵データを用いてそれぞれ暗号化された前記コンテンツ鍵データおよび前記権利書データを格納した前記モジュールを前記データ処理装置に配給する

請求項41に記載のデータ提供装置。

4.4. 所定の権威機関が発行した前記配信用鍵データを用いて、前記コンテンツ鍵データKcおよび前記権利書データを暗号化する

請求項43に記載のデータ提供装置。

45. 前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つに対して自らの署名データを作成し、当該作成した署名データを格納した前記モジュールを前記データ処理装置に配給する

請求項41に記載のデータ提供装置。

46. 自らの秘密鍵データを用いて前記署名データを作成し、当該秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する

請求項45に記載のデータ提供装置。

47. 前記公開鍵データの正当性を証明する公開鍵証明書データをを格納した 前記モジュールを前記データ処理装置に配給する

請求項46に記載のデータ提供装置。

48. 前記コンテンツデータを格納した第1のファイルと、

前記コンテンツ鍵データおよび前記権利書データを格納した第2のファイルとを格納した前記モジュールを前記データ処理装置に配給する

請求項41に記載のデータ提供装置。

49. 前記第1のファイルおよび前記第2のファイルについて、自らの秘密鍵 データを用いた署名データをそれぞれ作成し、当該作成した署名データを格納し た前記モジュールを前記データ処理装置に配給する

請求項48に記載のデータ提供装置。

50. 前記秘密鍵データに対応する公開鍵データを格納した前記モジュールを 前記データ処理装置に配給する

請求項49に記載のデータ提供装置。

5 1. 前記データ処理装置との間で相互認証を行い、当該相互認証によって得たセッション鍵データを用いて前記モジュールを暗号化し、当該暗号化したモジュールを前記データ処理装置に送信する

請求項41に記載のデータ提供装置。

- 5 2. 前記モジュールを記録した記録媒体を作成する 請求項41に記載のデータ提供装置。
- 5 3. 前記モジュールをアプリケーション層で定義する 請求項 4 1 に記載のデータ提供装置。
- 5 4. 前記モジュールを前記データ処理装置に配給する配送プロトコルとして 、前記アプリケーション層の下層のプレゼンテーション層およびトランスポート 層を用いる

請求項53に記載のデータ提供装置。

5.5. 前記モジュールを前記データ処理装置に配給するための媒体に依存しない形式で前記モジュールを定義する

請求項41に記載のデータ提供装置。

5 6. データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供方法において、

前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納

された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した 権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

57. 前記データ提供装置から前記データ処理装置に、配信用鍵データを用いてそれぞれ暗号化された前記コンテンツ鍵データおよび前記権利書データを格納した前記モジュールを配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを前記配信用鍵データを 用いて復号する

請求項56に記載のデータ提供方法。

5 8. データ提供装置、データ配給装置およびデータ処理装置を用いたデータ 提供方法において、

前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを提供し、

前記データ配給装置から前記データ処理装置に、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを配給し、

前記データ処理装置において、前記配給を受けた前記第2のモジュール に格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復 号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

5 9. 前記データ配給装置から前記データ処理装置に、前記コンテンツデータ の価格を示す価格データを格納した前記第 2 のモジュールを配給する

請求項58に記載のデータ提供方法。

60. データ提供装置と、少なくとも第1のデータ配給装置および第2のデータ配給装置と、データ処理装置とを用いたデータ提供方法において、

前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを提供し、

前記第1のデータ配給装置から前記データ処理装置に、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを配給し、

前記第2のデータ配給装置から前記データ処理装置に、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第3のモジュールを配給し、

前記データ処理装置において、前記配給を受けた前記第2のモジュール および前記第3のモジュールに格納された前記コンテンツ鍵データおよび前記権 利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

61.少なくとも第1のデータ提供装置および第2のデータ提供装置と、データ配給装置と、データ処理装置とを用いたデータ提供方法において、

前記第1のデータ提供装置から前記データ配給装置に、第1のコンテンツ鍵データを用いて暗号化された第1のコンテンツデータと、暗号化された前記第1のコンテンツ鍵データと、前記第1のコンテンツデータの取り扱いを示す暗号化された第1の権利書データとを格納した第1のモジュールを提供し、

前記第2のデータ提供装置から前記データ配給装置に、第2のコンテンツ鍵データを用いて暗号化された第2のコンテンツデータと、暗号化された前記第2のコンテンツ鍵データと、前記第2のコンテンツデータの取り扱いを示す暗

号化された第2の権利書データとを格納した第2のモジュールを提供し、

前記データ配給装置から前記データ処理装置に、前記提供を受けた前記第1のモジュールに格納された前記暗号化された前記第1のコンテンツデータ、前記第1のコンテンツ鍵データおよび前記第1の権利書データと、前記提供を受けた前記第2のモジュールに格納された前記暗号化された前記第2のコンテンツデータ、前記第2のコンテンツ鍵データおよび前記第2の権利書データとを格納した第3のモジュールを配給し、

前記データ処理装置において、前記配給を受けた前記第3のモジュールに格納された前記第1のコンテンツ鍵データおよび前記第1の権利書データを復号し、当該復号した第1の権利書データに基づいて、前記第1のコンテンツデータの取り扱いを決定し、前記配給を受けた前記第3のモジュールに格納された前記第2のコンテンツ鍵データおよび前記第2の権利書データを復号し、当該復号した第2の権利書データに基づいて、前記第2のコンテンツデータの取り扱いを決定する

データ提供方法。

62. コンテンツデータの利用を行うデータ処理装置に、前記コンテンツデータを配給するデータ提供方法において、

コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号 化された権利書データとを格納したモジュールを前記データ処理装置に配給する

データ提供方法。

63. 配信用鍵データを用いてそれぞれ暗号化された前記コンテンツ鍵データおよび前記権利書データを格納した前記モジュールを前記データ処理装置に配給する

請求項62に記載のデータ提供方法。

6.4. 前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書デー

タの少なくとも一つに対して自らの署名データを作成し、当該作成した署名データを格納した前記モジュールを前記データ処理装置に配給する

請求項62に記載のデータ提供方法。

65. 自らの秘密鍵データを用いて前記署名データを作成し、当該秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する

請求項64に記載のデータ提供方法。

66. 前記公開鍵データの正当性を証明する公開鍵証明書データをを格納した前記モジュールを前記データ処理装置に配給する

請求項65に記載のデータ提供方法。

67、前記コンテンツデータを格納した第1のファイルと、

前記コンテンツ鍵データおよび前記権利書データを格納した第2のファイルとを格納した前記モジュールを前記データ処理装置に配給する

請求項62に記載のデータ提供方法。

68. 前記第1のファイルおよび前記第2のファイルについて、自らの秘密鍵 データを用いた署名データをそれぞれ作成し、当該作成した署名データを格納し た前記モジュールを前記データ処理装置に配給する

請求項67に記載のデータ提供方法。

69. 前記秘密鍵データに対応する公開鍵データを格納した前記モジュールを 前記データ処理装置に配給する

請求項68に記載のデータ提供方法。

70. 前記データ処理装置との間で相互認証を行い、当該相互認証によって得たセッション鍵データを用いて前記モジュールを暗号化し、当該暗号化したモジュールを前記データ処理装置に送信する

請求項62に記載のデータ提供方法。

7 1. 前記モジュールを記録した記録媒体を作成する

請求項62に記載のデータ提供方法。

72. データ提供装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ処理装置に配給し、前記権利書データの正当性を証明することを前記管理装置に要求し、

前記データ処理装置は、前記配給を受けた権利書データに基づいて前記 配給を受けた前記コンテンツデータの利用を行い、

前記管理装置は、前記データ提供装置および前記データ処理装置を管理 し、前記データ提供装置からの要求に応じて、前記権利書データの正当性を証明 する

データ提供システム。

73. 前記データ提供装置は、前記権利書データと、自らの識別子と、少なくとも前記権利書データに対して自らの秘密鍵データを用いて作成した署名データとを格納したモジュールを前記管理装置に送信して前記要求を行う

請求項72に記載のデータ提供システム。

7.4. 前記管理装置は、前記データ提供装置の前記秘密鍵データに対応する公開鍵データの正当性を証明する公開鍵証明書データを、自らの秘密鍵データを用いて作成した署名データと共に、前記データ提供装置に配給し、

前記データ提供装置は、前記公開鍵証明書データと、前記権利書データと、自 らの識別子と、前記署名データとを格納したモジュールを前記管理装置に送信し て前記要求を行う

請求項73に記載のデータ提供システム。

75. 前記管理装置は、配信鍵データを管理し、当該配信鍵データを前記データ処理装置に配給し、前記データ提供装置からの要求に応じて、前記権利書データに対して自らの秘密鍵データを用いて作成した署名データを生成し、当該生成

した署名データと前記権利書データとを格納したモジュールを前記配信鍵データ を用いて暗号化して前記データ提供装置に送信し、

前記データ提供装置は、前記管理装置から受信したモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記データ提供装置から受信した前記モジュールを、 前記配信鍵データを用いて復号し、当該モジュールに格納された前記署名データ の正当性を前記管理装置の公開鍵データを用いて検証し、正当であると判断した 場合に、前記モジュールに格納された権利書データに基づいて前記配給を受けた 前記コンテンツデータの利用を行う

請求項72に記載のデータ提供システム。

76. 前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理 装置における前記コンテンツデータの前記購入および前記利用に伴って得られた 利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う

請求項72に記載のデータ提供システム。

77. データ提供装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを前記データ処理装置に配給し、前記コンテンツ鍵データの正当性を証明することを前記管理装置に要求し、

前記データ処理装置は、前記配給を受けたコンテンツデータを、前記コンテンツ鍵データを用いて復号し、当該復号したコンテンツデータを利用し、

前記管理装置は、前記データ提供装置および前記データ処理装置を管理

し、前記データ提供装置からの要求に応じて、前記コンテンツ**鍵**データの正当性 を証明する

データ提供システム。

78. 前記データ提供装置は、前記コンテンツデータおよび前記コンテンツ鍵 データを格納したモジュールを、前記データ処理装置に配給する

請求項77に記載のデータ提供システム。

79. コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを配給するデータ提供装置と、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行うデータ処理装置とを管理する管理装置であって、

前記データ提供装置からの要求に応じて、前記権利書データの正当性を 証明する

管理装置。

80. 前記データ提供装置から、前記権利書データと、当該データ提供装置の 識別子と、少なくとも前記権利書データに対して当該データ提供装置の秘密鍵デ ータを用いて作成した署名データとを格納したモジュールを用いた前記要求を受 ける場合に、

前記データ提供装置の秘密鍵データに対応する公開鍵データを管理する 請求項79に記載の管理装置。

8 1. 前記公開鍵データの正当性を証明する公開鍵証明書データを前記データ 提供装置に送信する

請求項80に記載の管理装置。

82. コンテンツ鍵データを用いて暗号化したコンテンツデータ、および当該 コンテンツデータの取り扱いを示す権利書データを配給するデータ提供装置と、 前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデー タを前記コンテンツ鍵データを用いて復号した後に当該コンテンツデータの利用

を行うデータ処理装置とを管理する管理装置であって、

前記データ提供装置からの要求に応じて、前記コンテンツ鍵データの正 当性を証明する

管理装置。

83. データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記権利書データの正当性を証明することを前記管理装置に要求し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記権 利書データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた権利書データに基づいて前記 配給を受けた前記コンテンツデータの利用を行い、

前記管理装置は、前記データ提供装置および前記データ処理装置を管理 し、前記データ提供装置からの要求に応じて、前記権利書データの正当性を証明 する

データ提供システム。

8 4. 前記データ提供装置は、前記コンテンツデータの識別子と、前記権利書 データと、少なくとも前記権利書データに対して自らの秘密鍵データを用いて作 成した署名データとを格納したモジュールを前記管理装置に送信して前記要求を 行う

請求項83に記載のデータ提供システム。

8 5. 前記管理装置は、前記データ提供装置の前記秘密鍵データに対応する公開鍵データの正当性を証明する公開鍵証明書データを、自らの秘密鍵データを用いて作成した署名データと共に、前記データ提供装置に配給する

請求項84に記載のデータ提供システム。

86. 前記管理装置は、配信鍵データを管理し、当該配信鍵データを前記データ処理装置に配給し、前記データ提供装置からの要求に応じて、前記権利書データに対して自らの秘密鍵データを用いて作成した署名データを生成し、当該生成した署名データと前記権利書データとを格納したモジュールを前記配信鍵データを用いて暗号化して前記データ提供装置に送信し、

前記データ提供装置は、前記管理装置から受信したモジュールを前記データ配給装置に提供し、

前記データ処理装置は、前記データ配給装置から配給を受けた前記モジュールを、前記配信鍵データを用いて復号し、当該モジュールに格納された前記署名データの正当性を前記管理装置の公開鍵データを用いて検証し、正当であると判断した場合に、前記モジュールに格納された権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行う

請求項83に記載のデータ提供システム。

87. 前記データ配給装置は、前記配給するコンテンツデータの価格を示す価格データを前記データ処理装置に配給し、

前記管理装置は、前記データ配給装置からの要求に応じて、前記価格データの正当性を証明する

請求項83に記載のデータ提供システム。

88. 前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理 装置における前記コンテンツデータの前記購入および前記利用に伴って得られた 利益を、前記データ提供装置および前記データ配給装置の関係者に分配するため の利益分配処理を行う

請求項83に記載のデータ提供システム。

89. 前記データ処理装置は、前記データ配給装置と通信を行う第1のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第2のモジュールとを有し、

前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う

請求項83に記載のデータ提供システム。

90. データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記コンテンツ鍵データおよび前記コンテンツ鍵データの正当性を証明することを前記管理装置に要求し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記権 利書データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた権利書データに基づいて、前 記コンテンツ鍵データを用いた前記コンテンツデータの復号を含む前記コンテン ツデータの利用を行い、

前記管理装置は、前記データ提供装置および前記データ処理装置を管理

し、前記データ提供装置からの要求に応じて、前記コンテンツ**鍵**データの正当性 を証明する

データ提供システム。

9 1. 前記データ提供装置は、前記コンテンツ鍵データを暗号化し、当該暗号 化したコンテンツ鍵データと前記暗号化したコンテンツデータとを格納したモジュールを前記データ配給装置に提供する

請求項90に記載のデータ提供システム。

92. コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを提供するデータ提供装置と、前記提供を受けた前記コンテンツデータおよび前記権利書データを配給するデータ配給装置と、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行うデータ処理装置とを管理する管理装置であって、

前記データ提供装置からの要求に応じて、前記権利書データの正当性を 証明する

管理装置。

93. 前記コンテンツデータをコンテンツ鍵データを用いて暗号化して前記データ提供装置から前記データ配給装置に提供する場合に、

前記データ提供装置からの要求に応じて、前記コンテンツ鍵データの正当性を 証明する

請求項92に記載の管理装置。

94. 前記価格データを前記コンテンツデータおよび前記権利書データと共に、前記データ配給装置から前記データ処理装置に配給する場合に、

前記データ配給装置からの要求に応じて、前記価格データの正当性を証明する 請求項92に記載の管理装置。

95. データ提供装置、データ処理装置および管理装置を用いたデータ提供方法において、

コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書デ ータとを前記データ提供装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた権利書データに基づい て前記配給を受けた前記コンテンツデータの利用を行い、

前記データ提供装置からの要求に応じて、前記管理装置において前記権 利書データの正当性を証明する

データ提供方法。

9 6. データ提供装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを 用いて暗号化したコンテンツデータを配給し、

前記データ処理装置において、前記配給を受けたコンテンツデータを、 前記コンテンツ鍵データを用いて復号し、当該復号したコンテンツデータを利用 し、

前記データ提供装置からの要求に応じて、前記管理装置において前記コンテンツ鍵データの正当性を証明する

データ提供方法。

97. データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ配給装置に、コンテンツデータと、 当該コンテンツデータの取り扱いを示す権利書データとを提供し、

前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを配給し、

前記データ処理装置において、前記配給を受けた権利書データに基づい て前記配給を受けた前記コンテンツデータの利用を行い、

前記データ提供装置からの要求に応じて、前記管理装置において、前記権利書

データの正当性を証明する

データ提供方法。

98. データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを 用いて暗号化したコンテンツデータと、当該コンテンツデータの取り扱いを示す 権利書データとを提供し、

前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた権利書データに基づいて、前記コンテンツ鍵データを用いた前記コンテンツデータの復号を含む前記コンテンツデータの利用を行い、

前記データ提供装置からの要求に応じて、前記管理装置において、前記 コンテンツ鍵データの正当性を証明する

データ提供方法。

99. データ提供装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータと、当該コンテンツデータの 取り扱いを示す権利書データとを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、前記データ提供装置および前記データ処理装置を管理 し、受信した前記履歴データに基づいて、前記データ処理装置における前記コン テンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提

供装置の関係者に分配するための利益分配処理を行う

データ提供システム。

100. 前記データ提供装置は、所定の鍵データを用いて前記コンテンツデータを暗号化して前記データ処理装置に配給し、

前記データ処理装置は、前記鍵データを用いて、前記受信したコンテンツデータを復号し、

前記管理装置は、前記鍵データを管理する

請求項99に記載のデータ提供システム。

101. 前記データ提供装置は、所定の鍵データを生成し、当該生成した鍵データを前記管理装置に登録し、

前記管理装置は、前記登録された前記鍵データを管理し、前記データ処理装置において、前記コンテンツデータの購入処理が行われたときに、対応する前記鍵データを前記データ処理装置に送信し、

前記データ処理装置は、受信した前記鍵データを用いて、前記受信した コンテンツデータを復号する

請求項99に記載のデータ提供システム。

102. 前記データ提供装置は、前記鍵データを暗号化し、当該暗号化した鍵データと前記暗号化したコンテンツデータと前記権利書データとを格納したモジュールを前記データ処理装置に配給する

請求項100に記載のデータ提供システム。

103. 前記管理装置は、配信用鍵データを管理し、前記配信用鍵データを前記データ提供装置および前記データ処理装置に配給し、

前記データ提供装置は、前記配信された前記配信用鍵データを用いて前 記鍵データおよび前記権利書データを暗号化し、

前記データ処理装置は、前記配信された前記配信用鍵データを用いて前 記鍵データおよび前記権利書データを復号する

請求項102に記載のデータ提供システム。

104. 前記管理装置は、各々所定の有効期限を持つ複数の前記配信用鍵データを、所定の期間分だけ、前記データ提供装置および前記データ処理装置に配給する

請求項103に記載のデータ提供システム。

105. 前記データ提供装置は、前記暗号化したコンテンツデータおよび前記権 利書データの少なくとも一方に対しての署名データを自らの秘密鍵データを用い て生成し、前記暗号化されたコンテンツデータ、前記暗号化した前記鍵データ、 前記暗号化された前記権利書データおよび前記署名データを格納したモジュール を前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュール内に格納された前記署名データを、前記秘密鍵データに対応する公開鍵データを用いて検証し

前記管理装置は、前記公開鍵データを管理する

請求項102に記載のデータ提供システム。

106. 前記データ提供装置は、前記自らの秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する

請求項105に記載のデータ提供システム。

107. 前記管理装置は、前記データ提供装置の前記秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する

請求項105に記載のデータ提供システム。

108. 前記管理装置は、前記データ提供装置および前記データ処理装置に、それぞれ配信鍵データを配給し、

前記データ提供装置は、前記権利書データを、前記配信鍵データを用いて暗号化して前記データ処理装置に配給し、

前記データ処理装置は、前記配信鍵データを用いて、受信した前記権利

## 書データを復号する

請求項99に記載のデータ提供システム。

109. 前記管理装置は、前記権利書データおよび前記鍵データの少なくとも一方の正当性を認証する

請求項100に記載のデータ提供システム。

110. 前記管理装置は、前記利益分配処理に応じた決済処理を行うことを請求する際に用いられる決済請求権データを生成し、当該決済請求権データに自らの秘密鍵データによる署名データを付加して、前記決済処理を行う装置あるいは前記データ提供装置に送信する

請求項99に記載のデータ提供システム。

111. 前記管理装置は、前記データ処理装置の登録処理を行い、登録された前 記データ処理装置を管理し、前記登録された前記データ処理装置から受信した前 記履歴データに基づいて前記利益分配処理を行う

請求項99に記載のデータ提供システム。

112. 前記データ処理装置は、前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態を決定し、当該決定した購入形態に応じた利用制御状態データを生成し、前記利用制御状態データに基づいて、前記配給を受けたコンテンツデータの利用を制御する

請求項99に記載のデータ提供システム。

113. 前記データ処理装置は、その処理内容、内部メモリに記憶された所定のデータおよび処理中のデータを、外部から監視および改竄困難なモジュールである

請求項99に記載のデータ提供システム。

114. コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを配給するデータ提供装置と、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一

方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを生成するデータ処理装置とを管理する管理装置であって、

前記履歴データを前記データ処理装置から受信し、当該受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を前記データ提供装置の関係者に分配するための利益分配処理を行う

管理装置。

115. 所定の鍵データを用いて暗号化した前記コンテンツデータを、前記データ提供装置から前記データ処理装置に配給する場合に、

前記鍵データを管理する

請求項113に記載の管理装置。

116. 前記権利書データと、前記コンテンツデータを前記暗号化する際に用いる鍵データとの少なくとも一方の正当性を認証する

請求項114に記載の管理装置。

117. コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとの配給をデータ提供装置から受け、当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益を前記データ提供装置の関係者に分配するための利益分配処理を所定の履歴データに基づいて行う管理装置に前記履歴データを送信するデータ処理装置であって、

前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す前記履歴データを前記管理装置に送信する

データ処理装置。

118. 前記コンテンツデータが所定の鍵データを用いて暗号化されている場合に、前記鍵データを前記データ提供装置から受ける

請求項117に記載のデータ処理装置。

119. 処理内容、内部メモリに記憶された所定のデータおよび処理中のデータを、外部から監視および改竄困難なモジュールを用いて構成される

請求項117に記載のデータ処理装置。

120. データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータと、当該コンテンツデータの 取り扱いを示す権利書データとを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記権 利書データを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置と通信を行う第1のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第2のモジュールとを有し、

前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う

データ提供システム。

121. 前記データ提供装置は、前記コンテンツデータを、コンテンツ鍵データを用いて暗号化して前記データ配給装置に提供する

請求項120に記載のデータ提供システム。

122. 前記データ配給装置は、前記配給するコンテンツデータの価格を示す価格データを作成し、当該価格データを前記データ処理装置に配給する

請求項120に記載のデータ提供システム。

123. 前記データ提供装置は、前記コンテンツ鍵データおよび前記権利書データを、配信鍵データを用いて暗号化して前記データ配給装置に提供し、

前記データ処理装置は、前記配信鍵データを用いて、前記コンテンツ鍵 データおよび前記権利書データを復号し、

前記管理装置は、前記配信鍵データを管理し、前記配信鍵データを前記データ提供装置および前記データ処理装置に配給する

請求項121に記載のデータ提供システム。

124. 前記データ提供装置は、前記暗号化されたコンテンツデータ、前記暗号化されたコンテンツ鍵データおよび前記暗号化された前記権利書データの少なくとも一つのデータに対しての第1の署名データを自らの第1の秘密鍵データを用いて生成し、前記暗号化されたコンテンツデータ、前記暗号化された鍵データ、前記暗号化された権利書データおよび前記第1の署名データを格納した第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記第1の秘密鍵データに対応する第1の公開 鍵データを用いて前記第1の署名データを検証した後に、自らの第2の秘密鍵デ ータを用いて生成した第2の署名データを前記第1のモジュールに格納して第2 のモジュールを生成し、当該第2のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記第1の公開鍵データを用いて、前記配給を 受けた前記第2のモジュールに格納された前記第1の署名データを検証し、前記 第2の秘密鍵データに対応する第2の公開鍵データを用いて、前記配給を受けた 前記第2のモジュールに格納された前記第2の署名データを検証し、

前記管理装置は、前記第1の公開鍵データおよび前記第2の公開鍵データを管理する

請求項123に記載のデータ提供システム。

125. 前記データ提供装置は、前記第1の公開鍵データを格納した前記第1の

モジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記第1の公開鍵データおよび前記第2の公開 鍵データを格納した前記第2のモジュールを前記データ処理装置に配給する

請求項124に記載のデータ提供システム。

126. 前記管理装置は、前記第1の公開鍵データおよび前記第2の公開鍵データを、前記データ処理装置に配給する

請求項124に記載のデータ提供システム。

127. 前記データ配給装置は、前記配給するコンテンツデータの価格を示す価格データを前記データ処理装置に配給し、

前記管理装置は、前記権利書データ、前記コンテンツデータを前記暗号 化する際に用いる鍵データおよび前記価格データのうち少なくとも一つのデータ の正当性を認証する

請求項120に記載のデータ提供システム。

128. 前記データ配給装置は、前記提供された暗号化されたコンテンツデータ、前記提供された権利書データ、前記コンテンツデータを暗号化した前記鍵データおよび前記配給されたコンテンツデータの価格を示す価格データとを格納したモジュールを、前記データ処理装置に配給する

請求項120に記載のデータ提供システム。

129. 前記管理装置は、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行って、決済を請求する際に用いられる決済請求権データを作成し、前記決済請求権データに自らの署名データを付加して、前記決済処理を行う装置に送信する

請求項120に記載のデータ提供システム。

130. 前記管理装置は、前記利益分配処理の結果を示す決済レポートデータを

、前記データ提供装置および前記データ配給装置の少なくとも一方に送信する 請求項129に記載のデータ提供システム。

131. 前記管理装置は、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行って、決済を請求する際に用いられる決済請求権データを作成し、前記決済請求権データに自らの署名データを付加して、前記データ提供装置および前記サービス提供装置の少なくとも一方に送信する請求項120に記載のデータ提供システム。

132. 前記管理装置は、前記データ処理装置の登録処理を行い、登録された前記データ処理装置を管理し、前記登録された前記データ処理装置から受信した前記履歴データに基づいて前記利益分配処理を行う

請求項120に記載のデータ提供システム。

133. 前記データ処理装置は、前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態に応じた利用制御状態データを生成し、前記利用制御状態データに基づいて、前記配給を受けたコンテンツデータの利用を制御する

請求項120に記載のデータ提供システム。

134. 前記データ処理装置の前記第2のモジュールは、その処理内容、予め内部に記憶されたデータおよび処理中のデータを、外部から監視および改竄困難なモジュールである

請求項120に記載のデータ提供システム。

135. コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを提供するデータ提供装置と、前記提供を受けた前記コンテンツデータおよび前記権利書データを配給するデータ配給装置と、前記配給を受けた前記権利書

データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用 形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なく とも一方の履歴を示す履歴データを生成するデータ処理装置とを管理する管理装 置であって、

受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う

管理装置。

136. 所定のコンテンツ鍵データを用いて暗号化した前記コンテンツデータを、前記データ提供装置から前記データ処理装置に配給する場合に、

前記鍵データを管理する

請求項135に記載の管理装置。

137. 前記権利書データおよび前記コンテンツ鍵データの少なくとも一方の正当性を認証する

請求項136に記載の管理装置。

138. コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとの提供をデータ提供装置から受けたデータ配給装置から、前記コンテンツデータおよび前記権利書データの配給を受け、当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を所定の履歴データに基づいて行う管理装置に前記履歴データを送信するデータ処理装置であって、

前記データ配給装置と通信を行う第1のモジュールと、

前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記 コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決 定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信す

る第2のモジュールと

を有するデータ処理装置。

139. 処理内容、内部メモリに記憶された所定のデータおよび処理中のデータを、外部から監視および改竄困難なモジュールからなる

請求項138に記載のデータ処理装置。

140. データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータと、当該コンテンツデータの 取り扱いを示す権利書データとを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記権 利書データを前記データ処理装置に配給し、前記データ処理装置から受信したデータ配給装置用購入履歴データに基づいて、前記コンテンツデータの配給に関する課金処理を行い、

前記データ処理装置は、前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信する第1のモジュールと、前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す管理装置用履歴データを前記管理装置に送信する第2のモジュールとを有し、

前記管理装置は、前記管理装置用履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴った得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配する利益分配処理を行う

データ提供システム。

141. コンテンツデータと当該コンテンツデータの取り扱いを示す権利書デー

タとの配給をデータ配給装置を介してデータ提供装置から受け、当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を前記管理装置用履歴データに基づいて行う管理装置に前記履歴データを送信するデータ処理装置であって、

前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信する第1のモジュールと、

前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記 コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決 定した購入形態および利用形態の履歴を示す前記管理装置用履歴データを前記管 理装置に送信する第2のモジュールと

を有するデータ処理装置。

142. データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記 データ処理装置によるデータ提供サービスの運用を管理する

データ提供システム。

143. 前記データ提供装置は、前記コンテンツデータの取り扱いを示す権利書 データを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび権利書 データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを、前 記配給を受けた前記権利書データに基づいて利用し、

前記管理装置は、ルート認証局に対して階層的に下に存在するサブ認証局の役割を果たし、登録された前記データ提供装置、前記データ配給装置および前記データ処理装置で用いられる秘密鍵データに対応する公開鍵データの正当性を証明する際に用いられる公開鍵証明書データの作成および管理と、前記権利書データの認証および前記コンテンツデータに関する権利処理とを行う

請求項142に記載のデータ提供システム。

144. 前記データ提供装置は、前記鍵データを用いて暗号化して前記データ配給装置に提供し、

前記管理装置は、前記鍵データを管理する

請求項143に記載のデータ提供システム。

1 4 5. 前記データ提供装置および前記データ配給装置の各々は、他の装置との間で認証を行う際に用いられる自らの秘密鍵データを作成し、当該作成した秘密鍵データを管理し、当該秘密鍵データに対応する公開鍵データを作成し、当該公開鍵データと身分証明書およひ決済口座を前記管理装置に登録し、

前記管理装置は、前記登録に応じて、前記公開鍵データの正当性を証明 する公開鍵証明書データを作成する。

請求項143に記載のデータ提供システム。

146. 前記管理装置は、前記登録に応じて、前記データ提供装置および前記データ配給装置に識別番号をそれぞれ割り振り、前記データ提供装置および前記データ配給装置に、ルート認証局の公開鍵データおよび管理装置の公開鍵データを 送信する

請求項145に記載のデータ提供システム。

147. 前記データ提供装置および前記データ配給装置の各々は、前記秘密鍵データをさらに前記管理装置に登録する

請求項145に記載のデータ提供システム。

148. 前記データ処理装置には、前記管理装置が生成した秘密鍵データおよび 当該秘密鍵データに対応する公開鍵データが予め格納されている

請求項143に記載のデータ提供システム。

149. 前記データ処理装置には、前記管理装置が生成した前記公開鍵データの正当性を証明する公開鍵証明書データが予め格納されている

請求項148に記載のデータ提供システム。

150. データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供 し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ 処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記 データ処理装置によるデータ提供サービスの運用を管理する

データ提供システムにおいて、

前記データ提供装置、前記データ配給装置、前記データ処理装置および 前記管理装置との間でのデータの伝送を、公開鍵暗号化方式を用いた相互認証、 署名生成、署名検証と、共通鍵暗号化方式によるデータの暗号化とを用いて行う

データ提供システム。

151. データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ 処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理する

データ提供システムにおいて、

前記データ提供装置、前記データ配給装置および前記データ処理装置は、他の装置との間で通信を行う前に、前記管理装置から自らの前記公開鍵証明書データを取得し、当該取得した公開鍵証明書データを前記他の装置に送信する

データ提供システム。

152. データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供 し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ 処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理する

データ提供システムにおいて、

前記データ提供装置、前記データ配給装置および前記データ処理装置は、他の装置との間で通信を行う際に、前記管理装置から自らの前記公開鍵証明書データを取得し、当該取得した公開鍵証明書データを前記通信時に前記他の装置に送信する

データ提供システム。

153. データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ 処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記

データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、前記データ提供装置、前記データを特定する公開鍵証明書破棄データを生成し、前記データ提供装置、前記データ配給装置および前記データ処理装置が前記公開鍵証明書破棄データが特定する公開鍵証明書データを用いた前記通信または前記配給を行うことを規制する

データ提供システム。

154. 前記管理装置は、不正行為に用いられた前記データ提供装置、前記データ配給装置および前記データ処理装置に対応する公開鍵証明書データを特定する前記公開鍵証明書破棄データを生成する

請求項153に記載のデータ提供システム。

155. データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供 し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ 処理装置に配給し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記 データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置 が、他の装置にデータを供給するときに、当該データが自らによって作成された

ことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ提供装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記管理装置から前記配給を受けた公開鍵証明 書破棄データに基づいて、前記配給を受けたコンテンツデータを提供した前記データ提供装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記配給を受けたコンテンツデータの利用を制御する

データ提供システム。

156. 前記管理装置は、前記公開鍵証明書破棄データを前記データ処理装置に直接配給する

請求項155に記載のデータ提供システム。

157. 前記管理装置は、前記公開鍵証明書破棄データを、前記データ配給装置を介して、放送あるいはオンデマンド方式で前記データ処理装置に配給する

請求項155に記載のデータ提供システム。

158. データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ提供装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効に

する公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開 鍵証明書破棄データを前記データ配給装置に配給し、

前記データ配給装置は、前記管理装置から前記配給を受けた公開鍵証明 書破棄データに基づいて、前記提供を受けたコンテンツデータを提供した前記データ提供装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記提供されたコンテンツデータの前記データ処理装置への配給を制御する

データ提供システム。

159. データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、

前記データ提供装置は、前記管理装置から前記配給を受けた公開鍵証明 書破棄データに基づいて、コンテンツデータの提供先のデータ配給装置の公開鍵 証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記データ配給装置への前記コンテンツデータの提供を制御する

前記データ配給装置は、前記提供されたコンテンツデータを前記データ 処理装置に配給し、

前記データ処理装置は、前記配給を受けたコンテンツデータを利用する

データ提供システム。

160. データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記 データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置 が、他の装置にデータを供給するときに、当該データが自らによって作成された ことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署 名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する 場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証 明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効に する公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開 鍵証明書破棄データを前記データ配給装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータの提供し、

前記データ配給装置は、前記提供されたコンテンツデータと、前記配給 を受けた公開鍵証明書破棄データとを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御する

データ提供システム。

161. 前記データ配給装置は、前記管理装置から配給を受けた前記公開鍵証明 書破棄データを改竄困難な構成を有している

請求項160に記載のデータ提供システム。

162. 前記管理装置は、前記公開鍵証明書破棄データを配信用鍵データを用いて暗号化して前記データ配給装置に配給し、前記配信用鍵データを前記データ処

理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データを前 記配信用鍵データを用いて復号する

請求項160に記載のデータ提供システム。

163. 前記データ配給装置は、前記公開鍵証明書破棄データを、放送あるいはオンデマンド方式で前記データ処理装置に配給する

請求項160に記載のデータ提供システム。

164. データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータを提供 し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ 処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御する

データ提供システム。

165. データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータおよび 前記公開鍵証明書破棄データを提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび公開鍵 証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御する

データ提供システム。

166. データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記 データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置 が、他の装置にデータを供給するときに、当該データが自らによって作成された

ことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ処理装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータおよび 前記公開鍵証明書破棄データを提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび公開鍵 証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置から配給を受けた公開鍵証明書破棄データに基づいて他のデータ処理装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記他のデータ処理装置との間の通信を制御する

データ提供システム。

167. 前記データ配給装置は、前記管理装置から配給を受けた前記公開鍵証明書破棄データを改竄困難な構成を有している

請求項166に記載のデータ提供システム。

168. 前記管理装置は、前記公開鍵証明書破棄データを配信用鍵データを用いて暗号化して前記データ提供装置に配給し、前記配信用鍵データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データを前 記配信用鍵データを用いて復号する

請求項166に記載のデータ提供システム。

169. データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ処理装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータを提供 し、

前記データ配給装置は、前記提供されたコンテンツデータと、前記配給された公開鍵証明書破棄データとを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置から配給を受けた公開鍵証明書破棄データに基づいて他のデータ処理装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記他のデータ処理装置との間の通信を制御する

データ提供システム。

170. 前記データ配給装置は、前記管理装置から配給を受けた前記公開鍵証明 書破棄データを改竄困難な構成を有している

請求項169に記載のデータ提供システム。

171. 前記管理装置は、前記公開鍵証明書破棄データを配信用鍵データを用いて暗号化して前記データ配給装置に配給し、前記配信用鍵データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データを前 記配信用鍵データを用いて復号する

請求項169に記載のデータ提供システム。

172. データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、

前記データ処理装置は、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データを前記管理装置に供給し、前記管理装置から供給された登録データ内の破棄フラグを参照して、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データに基づいて、前記データ処理装置から供給を受けた前記登録データ内の前記破棄フラグを設定して新たな登録データを生成し、当該生成した登録データを前記データ処理装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータを提供 し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ 処理装置に配給する

データ提供システム。

173. データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記

データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータおよび 前記公開鍵証明書破棄データを提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記公 開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データ内の破棄フラグを設定し、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制する

データ提供システム。

174. データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記 データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置 が、他の装置にデータを供給するときに、当該データの正当性を示す署名データ を自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公 開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明 書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄デー タを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータを提供

し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記公 開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データ内の破棄フラグを設定し、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制する

データ提供システム。

175. データ提供装置、データ配給装置、データ処理装置および管理装置を有 するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータと、当該コンテンツデータの 取り扱いを示す権利書データとを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記権 利書データを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置と通信を行う第1のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第2のモジュールとを有し、

前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、

前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処

理を行い、当該利益分配処理の結果に基づいて決済を行う決済機能と、前記権利 書データの登録を行う権利管理機能とを有する

データ提供システム。

176. 前記管理装置は、

前記決済機能を有する第1の管理装置と、

前記権利管理機能を有する第2の管理装置と

を有する

請求項175に記載のデータ提供システム。

177.前記決済は、電子決済である

請求項175に記載のデータ提供システム。

178. データ提供装置、データ配給装置、データ処理装置および管理装置を有 するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータと、当該コンテンツデータの 取り扱いを示す権利書データとを前記データ配給装置に提供し、

前記データ配給装置は、前記管理装置から配給を受けた決済請求権データを用いて決済処理を行う課金機能を有し、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置と通信を行う第1のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第2のモジュールとを有し、

前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、

前記第2のモジュールから受信した前記履歴データに基づいて、前記デ ータ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コ

ンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記 データ提供装置および前記データ配給装置の関係者に分配するための利益分配処 理を行い、当該利益分配処理の結果に基づいて決済を行う際に用いられる決済請 求権データを生成して前記データ配給装置に供給する決済請求権データ生成機能 と、前記権利書データの登録を行う権利管理機能とを有する

データ提供システム。

179. データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、前記管理装置から配給を受けた決済請求権データを用いて決済処理を行う課金機能を有し、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記権 利書データを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置と通信を行う第1のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第2のモジュールとを有し、

前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、

前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行い、当該利益分配処理の結果に基づいて決済を行う際に用いられる決済請求権データを生成して前記データ提供装置に配給する決済請求権データ生成機能

と、前記権利書データの登録を行う権利管理機能とを有する

データ提供システム。

180. データ提供装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ処理装置に、コンテンツデータと、 当該コンテンツデータの取り扱いを示す権利書データとを配給し、

前記データ処理装置において、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置において、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う

データ提供方法。

181. データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ配給装置に、コンテンツデータと、 当該コンテンツデータの取り扱いを示す権利書データとを提供し、

前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを配給し、

前記データ処理装置において、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置において、前記第2のモジュールから受信した前記履歴デ

ータに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う

データ提供方法。

182. データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ配給装置に、コンテンツデータと、 当該コンテンツデータの取り扱いを示す権利書データとを提供し、

前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、

前記データ処理装置において、前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信し、前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す管理装置用履歴データを前記管理装置に送信し、

前記管理装置において、前記管理装置用履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴った得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配し、

前記データ配給装置において、前記データ処理装置から受信したデータ 配給装置用購入履歴データに基づいて、前記コンテンツデータの配給に関する課 金処理を行う

データ提供方法。

183. データ提供装置、データ配給装置、データ処理装置および管理装置を用

いてコンテンツデータの提供を行うデータ提供方法であって、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供 し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ 処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記 データ処理装置によるデータ提供サービスの運用を管理する

データ提供方法において、

前記データ提供装置、前記データ配給装置、前記データ処理装置および 前記管理装置との間でのデータの伝送を、公開鍵暗号化方式を用いた相互認証、 署名生成、署名検証と、共通鍵暗号化方式によるデータの暗号化とを用いて行う データ提供方法。

184. データ提供装置、データ配給装置、データ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供 し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ 処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用 し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記 データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置 、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを 供給するときに、当該データが自らによって作成されたことを示す署名データを

自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、

前記データ提供装置、前記データ配給装置および前記データ処理装置は、他の装置との間で通信を行う前に、前記管理装置から自らの前記公開鍵証明書データを取得し、当該取得した公開鍵証明書データを前記他の装置に送信する

データ提供方法。

185. データ提供装置、データ配給装置、データ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供 し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ 処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、

前記データ提供装置、前記データ配給装置および前記データ処理装置は、他の装置との間で通信を行う際に、前記管理装置から自らの前記公開鍵証明書データを取得し、当該取得した公開鍵証明書データを前記通信時に前記他の装置に送信する

データ提供方法。

186. データ提供装置、データ配給装置、データ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供 し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ 処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、前記データ提供装置、前記データ配給装置および前記データ処理装置が前記公開鍵証明書破棄データが特定する公開鍵証明書データを用いた前記通信または前記配給を行うことを規制する

データ提供方法。

187. 前記管理装置は、不正行為に用いられた前記データ提供装置、前記データ配給装置および前記データ処理装置に対応する公開鍵証明書データを特定する前記公開鍵証明書破棄データを生成する

請求項186に記載のデータ提供方法。

188. データ提供装置、データ配給装置、データ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供 し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ提供装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記管理装置から前記配給を受けた公開鍵証明 書破棄データに基づいて、前記配給を受けたコンテンツデータを提供した前記データ提供装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記配給を受けたコンテンツデータの利用を制御する

データ提供方法。

189. 前記管理装置は、前記公開鍵証明書破棄データを前記データ処理装置に

## 直接配給する

請求項188に記載のデータ提供方法。

190. 前記管理装置は、前記公開鍵証明書破棄データを、前記データ配給装置を介して、放送あるいはオンデマンド方式で前記データ処理装置に配給する

請求項188に記載のデータ提供方法。

191. データ提供装置、データ配給装置、データ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ提供装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、

前記データ配給装置は、前記管理装置から前記配給を受けた公開鍵証明 書破棄データに基づいて、前記提供を受けたコンテンツデータを提供した前記デ ータ提供装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結 果に基づいて、前記提供されたコンテンツデータの前記データ処理装置への配給 を制御する

データ提供方法。

192. データ提供装置、データ配給装置、データ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記 データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置

が、他の装置にデータを供給するときに、当該データが自らによって作成された ことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署 名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する 場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証 明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効に する公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開 鍵証明書破棄データを前記データ提供装置に配給し、

前記データ提供装置は、前記管理装置から前記配給を受けた公開鍵証明 書破棄データに基づいて、コンテンツデータの提供先のデータ配給装置の公開鍵 証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記デ ータ配給装置への前記コンテンツデータの提供を制御し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ 処理装置に配給し、

> 前記データ処理装置は、前記配給を受けたコンテンツデータを利用する データ提供方法。

193. データ提供装置、データ配給装置、データ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記 データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置 が、他の装置にデータを供給するときに、当該データが自らによって作成された ことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署 名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する 場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証 明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効に する公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開 鍵証明書破棄データを前記データ配給装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータの提供 し、

前記データ配給装置は、前記提供されたコンテンツデータと、前記配給 を受けた公開鍵証明書破棄データとを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御する

データ提供方法。

194. 前記データ配給装置は、前記管理装置から配給を受けた前記公開鍵証明書破棄データを改竄困難な構成を有している

請求項193に記載のデータ提供方法。

195. 前記管理装置は、前記公開鍵証明書破棄データを配信用鍵データを用いて暗号化して前記データ配給装置に配給し、前記配信用鍵データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データを前 記配信用鍵データを用いて復号する

請求項193に記載のデータ提供方法。

196. 前記データ配給装置は、前記公開鍵証明書破棄データを、放送あるいはオンデマンド方式で前記データ処理装置に配給する

請求項160に記載のデータ提供方法。

197. データ提供装置、データ配給装置、データ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記 データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置 が、他の装置にデータを供給するときに、当該データが自らによって作成された

ことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータを提供 し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御する

データ提供方法。

198. データ提供装置、データ配給装置、データ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータおよび 前記公開鍵証明書破棄データを提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび公開鍵 証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御する

データ提供方法。

199. データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記 データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置 が、他の装置にデータを供給するときに、当該データが自らによって作成された ことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署 名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する 場合に、前記データ処理装置の秘密鍵データに対応する公開鍵データの公開鍵証 明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効に する公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開 鍵証明書破棄データを前記データ提供装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータおよび 前記公開鍵証明書破棄データを提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび公開鍵 証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置から配給を受けた公開鍵証 明書破棄データに基づいて他のデータ処理装置の公開鍵証明書データが無効であ

るか否かを検証し、当該検証の結果に基づいて前記他のデータ処理装置との間の 通信を制御する

データ提供方法。

200. 前記データ配給装置は、前記管理装置から配給を受けた前記公開鍵証明 書破棄データを改竄困難な構成を有している

請求項199に記載のデータ提供方法。

201. 前記管理装置は、前記公開鍵証明書破棄データを配信用鍵データを用いて暗号化して前記データ提供装置に配給し、前記配信用鍵データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データを前 記配信用鍵データを用いて復号する

請求項199に記載のデータ提供方法。

202. データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記 データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置 が、他の装置にデータを供給するときに、当該データが自らによって作成された ことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署 名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する 場合に、前記データ処理装置の秘密鍵データに対応する公開鍵データの公開鍵証 明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効に する公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開 鍵証明書破棄データを前記データ配給装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータを提供 し、

前記データ配給装置は、前記提供されたコンテンツデータと、前記配給

された公開鍵証明書破棄データとを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置から配給を受けた公開鍵証明書破棄データに基づいて他のデータ処理装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記他のデータ処理装置との間の通信を制御する

データ提供方法。

203. 前記データ配給装置は、前記管理装置から配給を受けた前記公開鍵証明書破棄データを改竄困難な構成を有している

請求項202に記載のデータ提供方法。

204. 前記管理装置は、前記公開鍵証明書破棄データを配信用鍵データを用いて暗号化して前記データ配給装置に配給し、前記配信用鍵データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データを前 記配信用鍵データを用いて復号する

請求項202に記載のデータ提供方法。

205. データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記データ処理装置は、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データを前記管理装置に供給し、前記管理装置から供給された登録データ内の破棄フラグを参照して、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記 データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置 が、他の装置にデータを供給するときに、当該データの正当性を示す署名データ を自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公

開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データに基づいて、前記データ処理装置から供給を受けた前記登録データ内の前記破棄フラグを設定して新たな登録データを生成し、当該生成した登録データを前記データ処理装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータを提供 し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ 処理装置に配給する

データ提供方法。

206. データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータおよび 前記公開鍵証明書破棄データを提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記公 開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、自らが接続された所定のネットワーク内に接続された既に登録された前

記データ処理装置を示す登録データ内の破棄フラグを設定し、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制する

データ提供方法。

207. データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記公 開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データ内の破棄フラグを設定し、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制する

データ提供方法。

208. データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供方法において、

前記データ提供装置は、前記管理装置から配給を受けた決済請求権デー

タを用いて決済処理を行う課金機能を有し、コンテンツデータと、当該コンテン ツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、

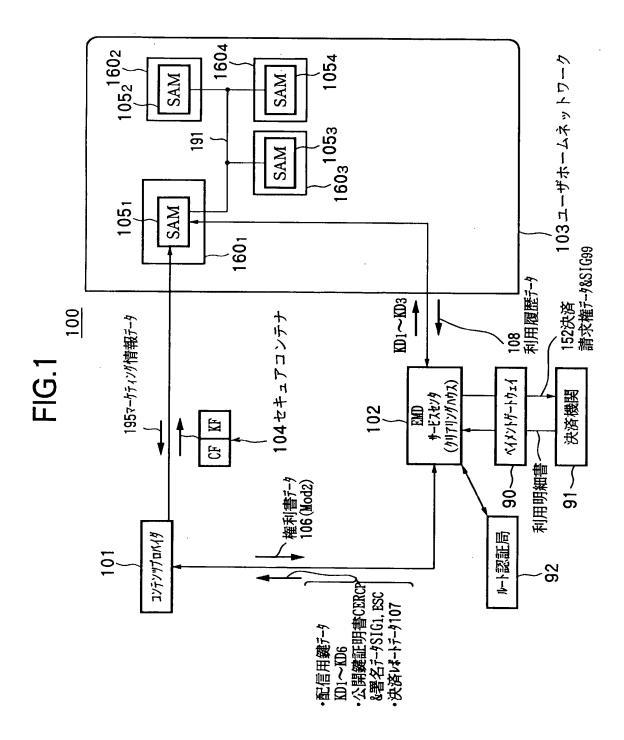
前記データ配給装置は、前記提供されたコンテンツデータおよび前記権 利書データを前記データ処理装置に配給し、

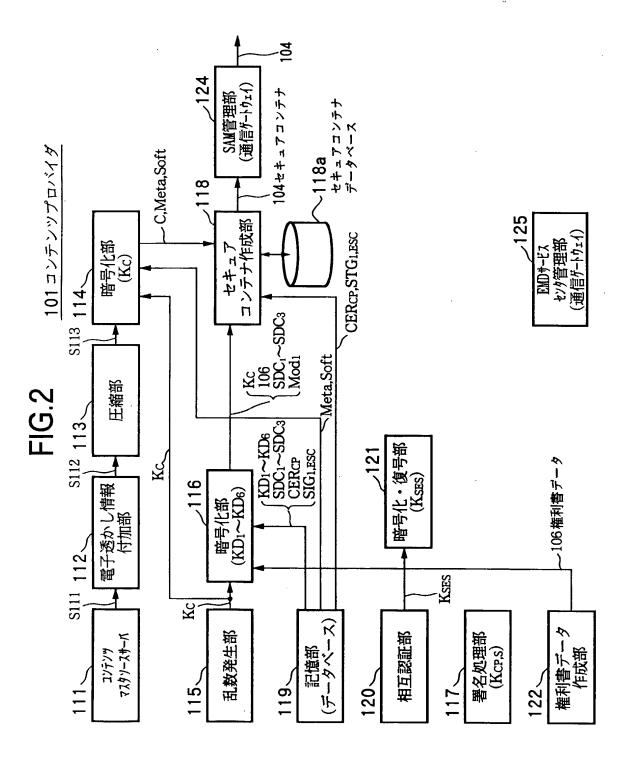
前記データ処理装置は、第1のモジュールによって前記データ配給装置 と通信を行い、第2のモジュールによって前記配給を受けた前記権利書データに 基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少 なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴 データを前記管理装置に送信し、

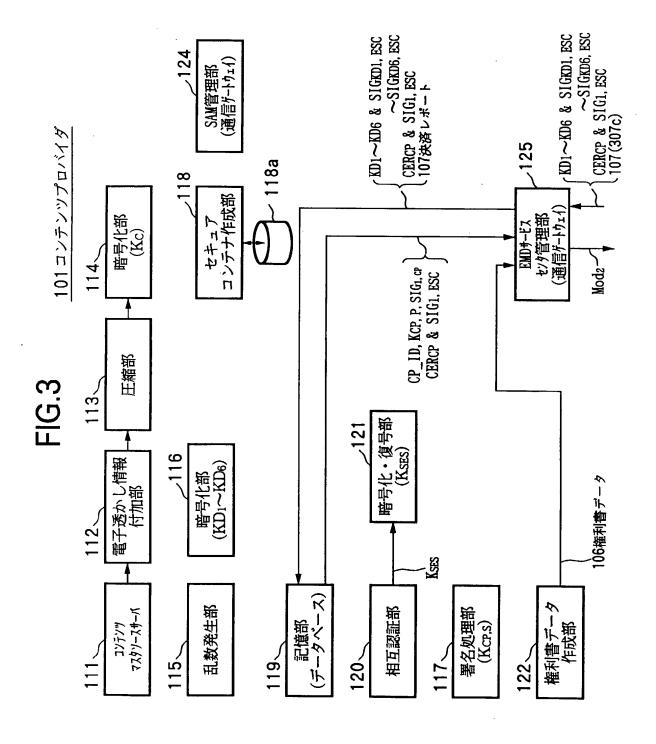
前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、

前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行い、当該利益分配処理の結果に基づいて決済を行う際に用いられる決済請求権データを生成して前記データ提供装置に配給し、、前記権利書データの登録を行う

データ提供方法。







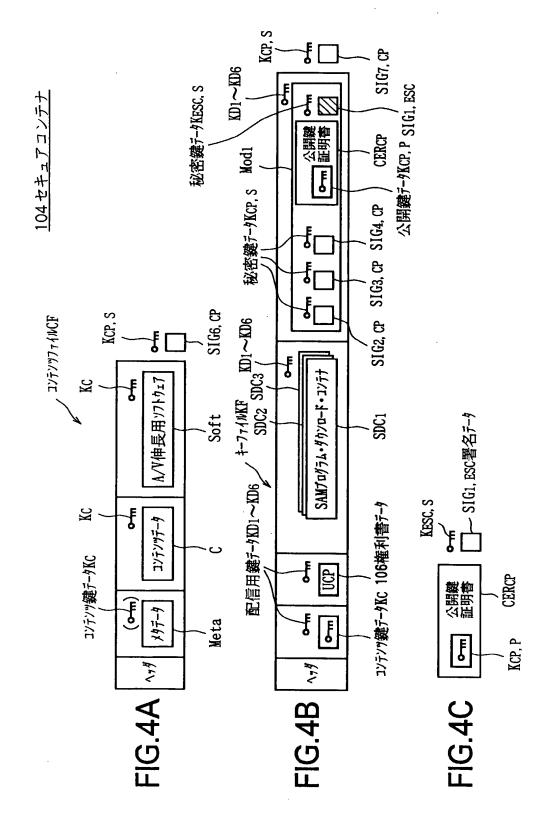
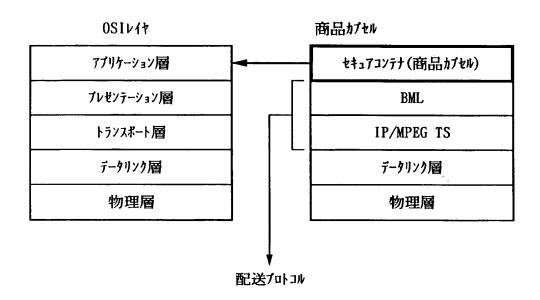
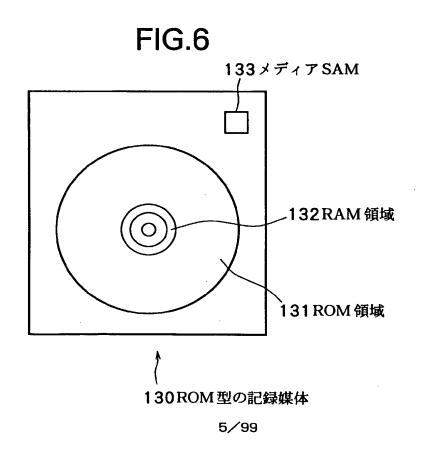
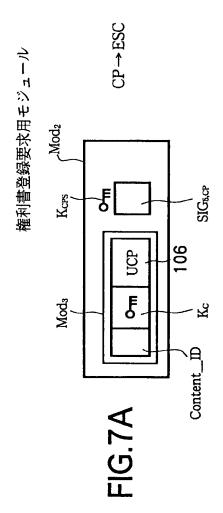


FIG.5







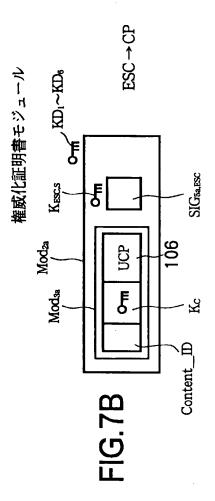
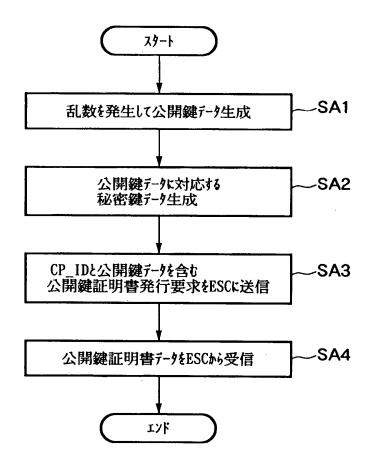
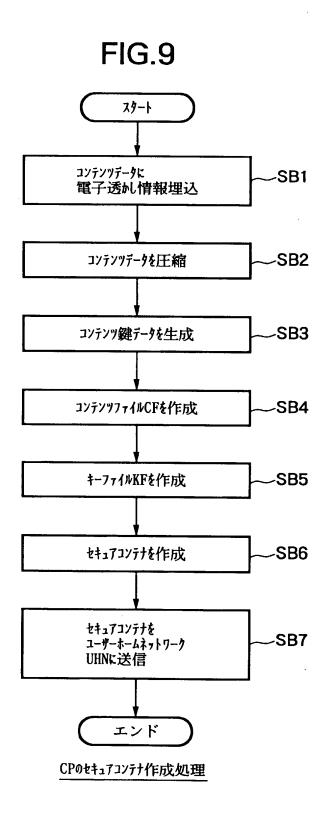


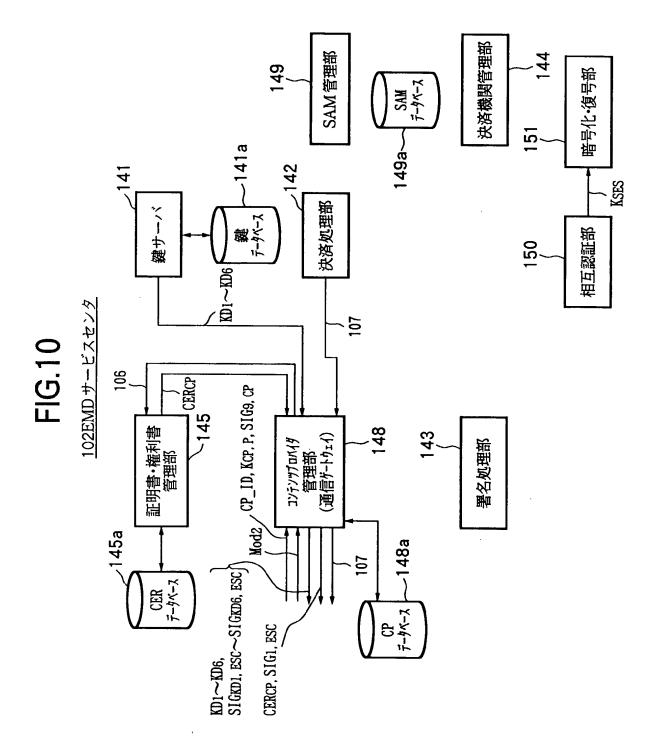
FIG.8



CPhiESCへの公開鍵証明書テータの発行要求処理



8/99



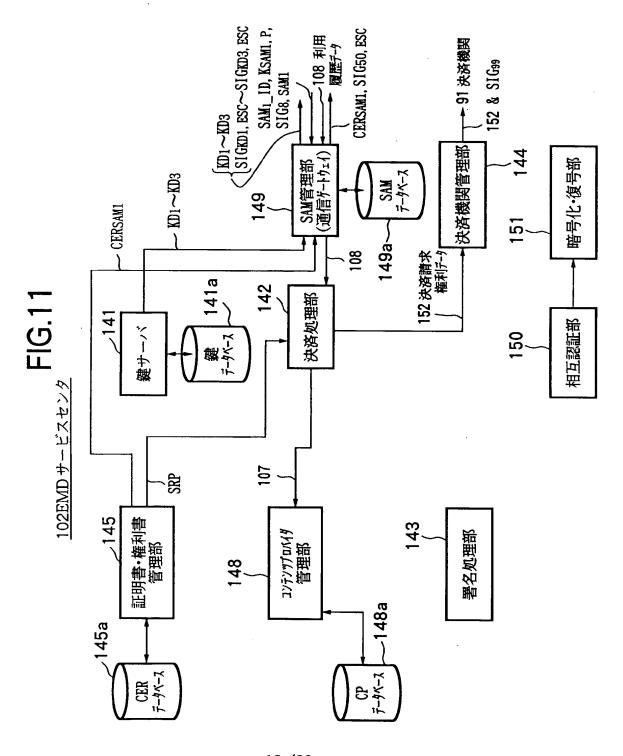
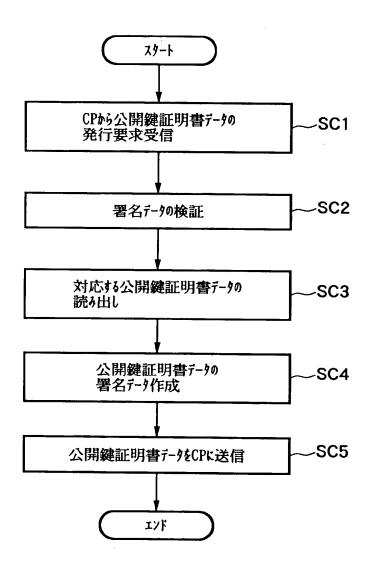
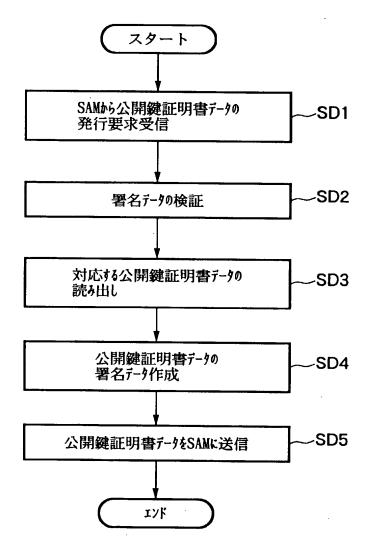


FIG.12



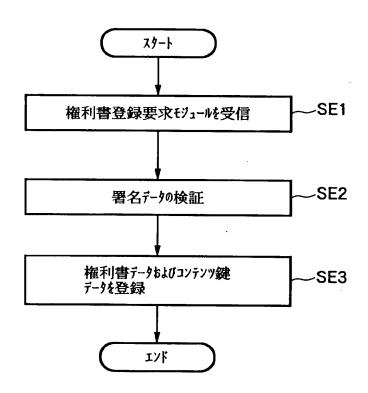
CPからの公開鍵証明書データの発行要求に応じたESCの処理

**FIG.13** 



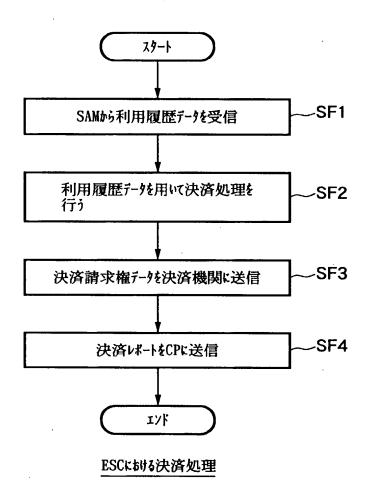
SAMからの公開鍵証明書データの発行要求に応じたESCの処理

**FIG.14** 

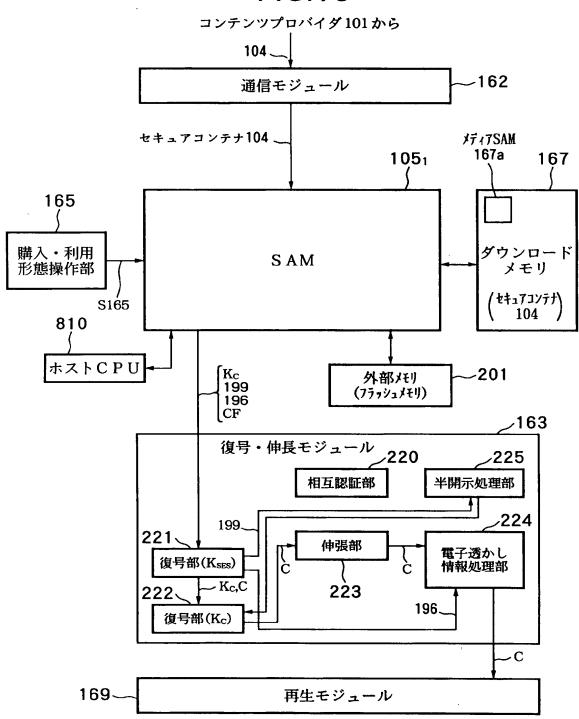


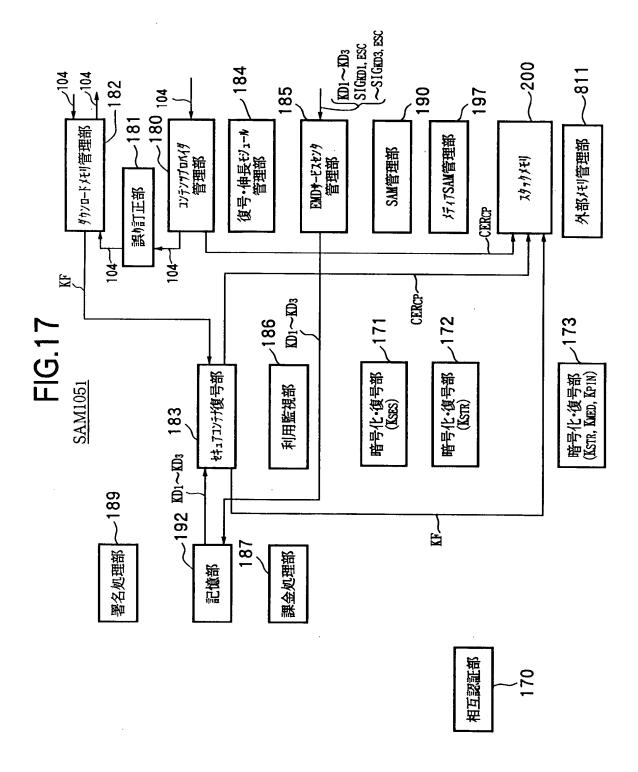
ESCにおける権利書データおよびコンテンツ鍵データの登録処理

**FIG.15** 



**FIG.16** 





## **FIG.18**

外部メモリ 201 に記憶されるデータ

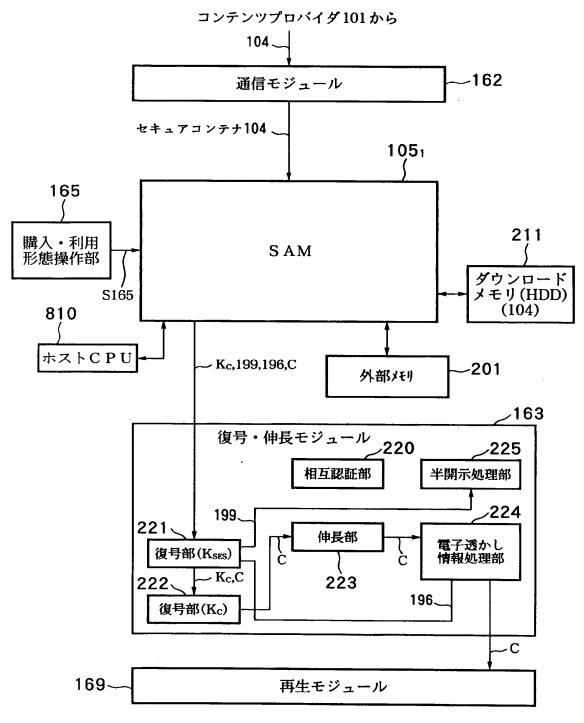
利用履歴データ 108 SAM 登録リスト

# **FIG.19**

#### スタックメモリ 200 に記憶されるデータ

コンテンツ鍵データ Kc 権利書データ (UCP) 106 記憶部 (フラッシュメモリ) 192 のロック鍵データ K<sub>LOC</sub> コンテンツプロバイダ 101 の公開鍵証明書 CER<sub>CP</sub> 利用制御情状態データ (UCS) 166 SAM プログラム・ダウンロード・コンテナ SD<sub>1</sub>~SDC<sub>3</sub>

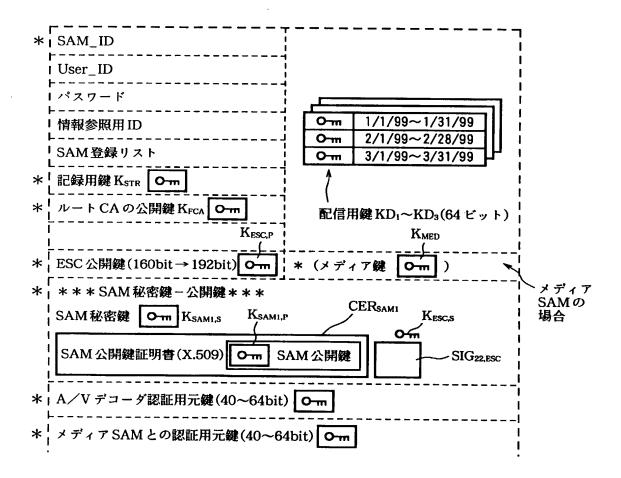
**FIG.20** 

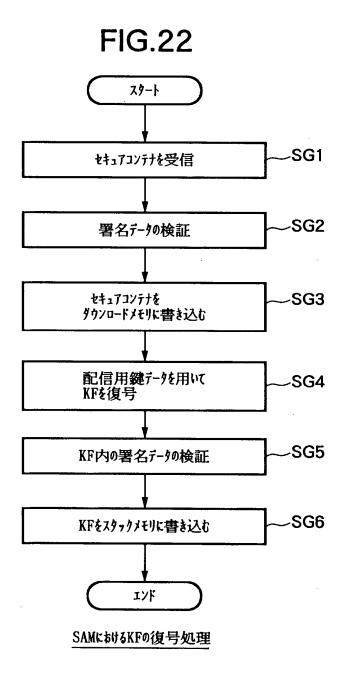


18/99

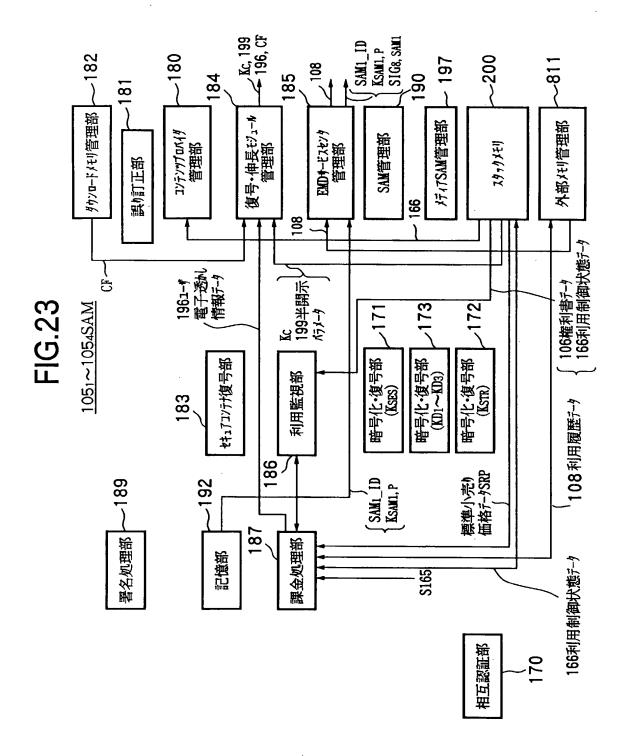
# FIG.21

#### 記憶部 192 に記憶されるデータ

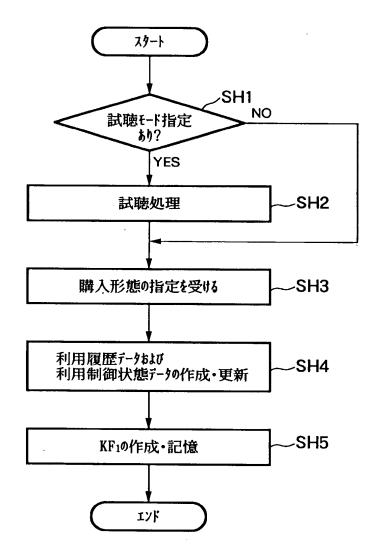




20/99

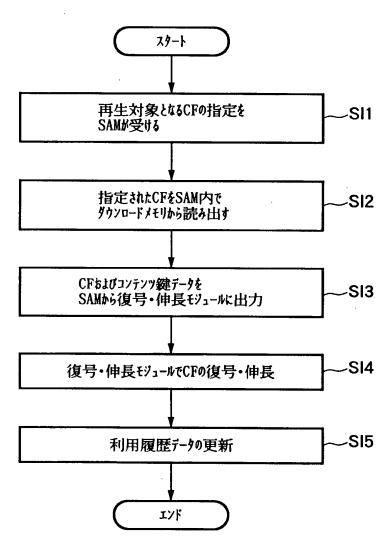


**FIG.24** 

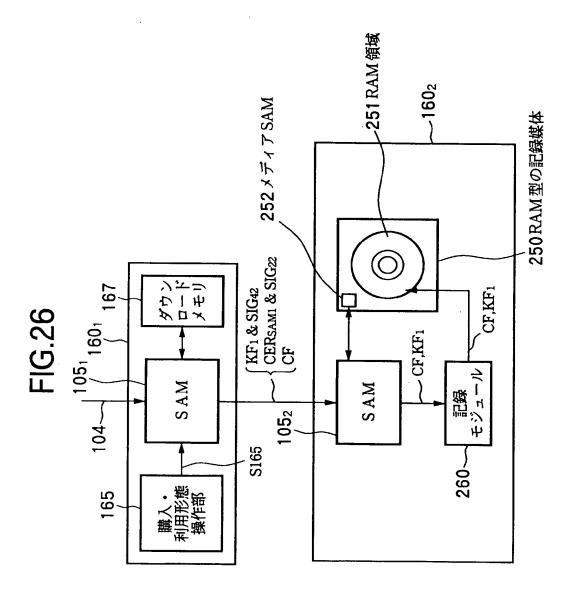


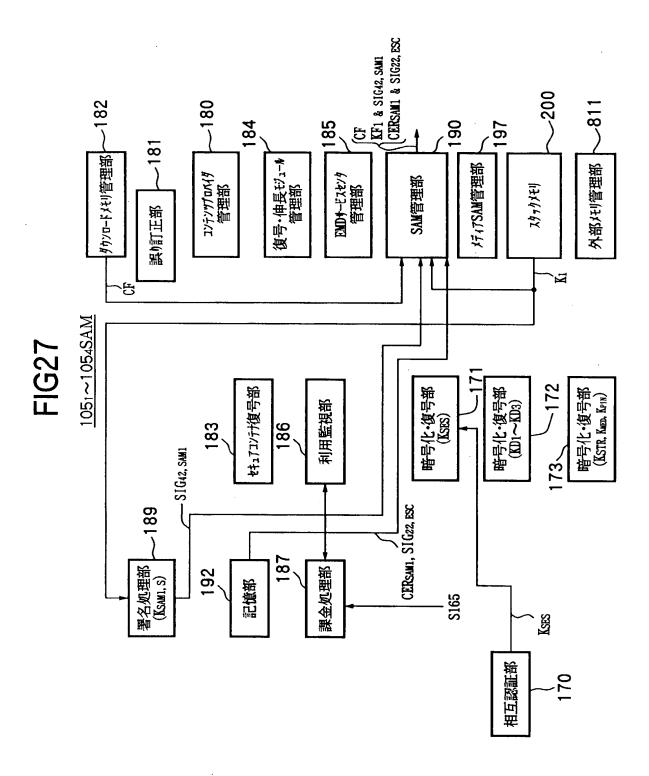
SAMにおけるセキュアコンテナの購入形態決定処理



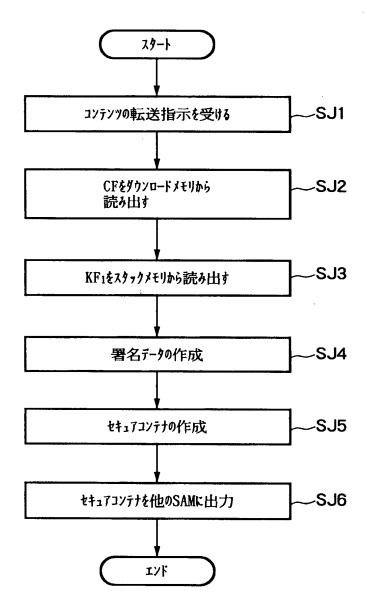


コンテンツデータの再生処理

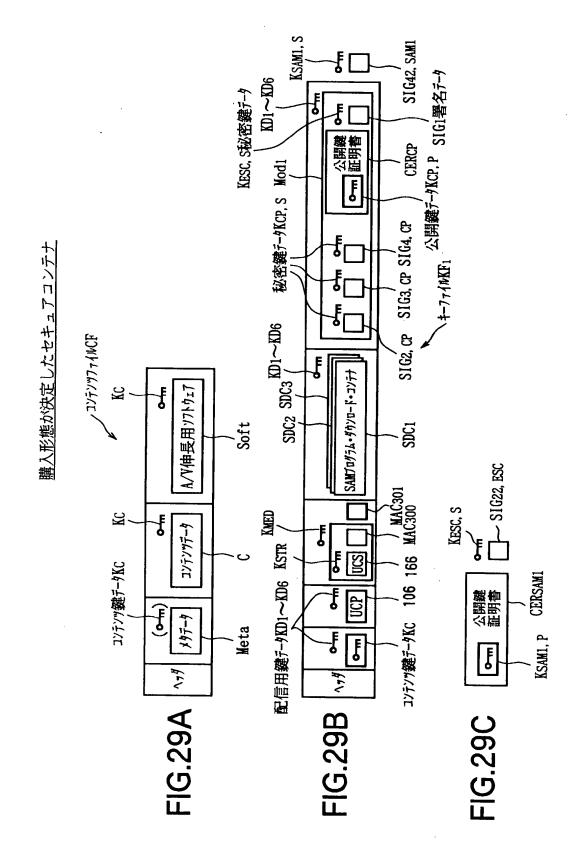




**FIG.28** 



購入形態決定後のコンテンツを他のSAMに転送するSAMの処理



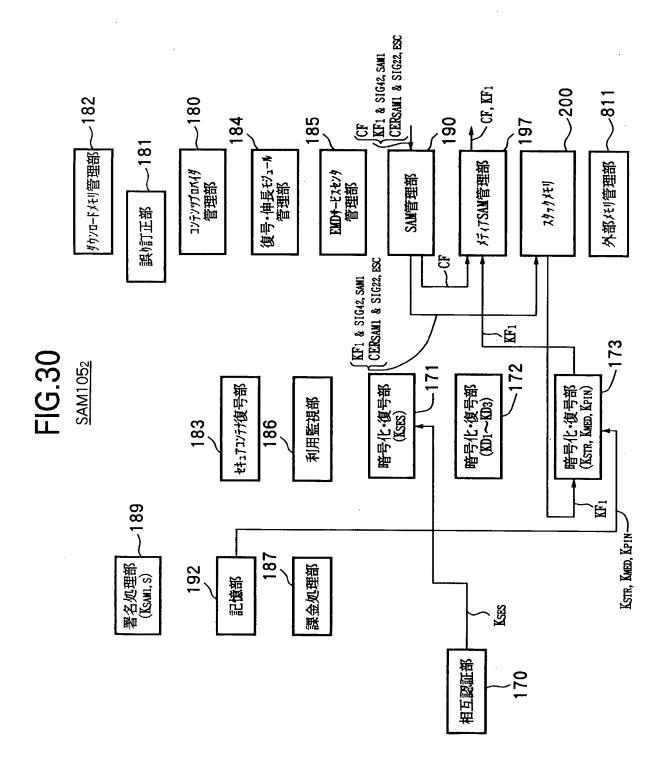
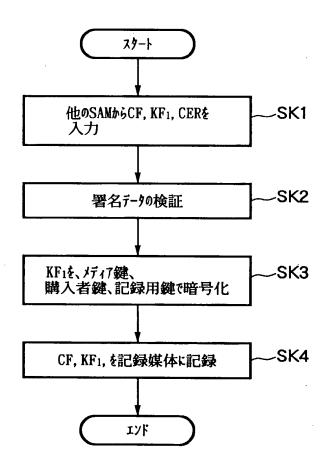
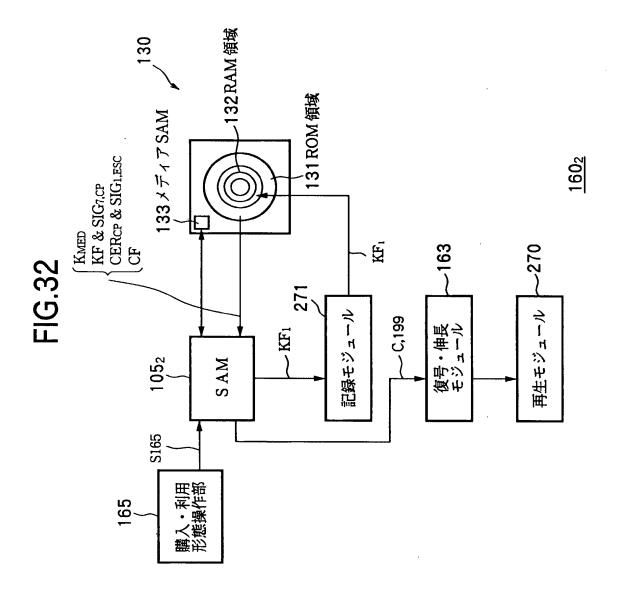
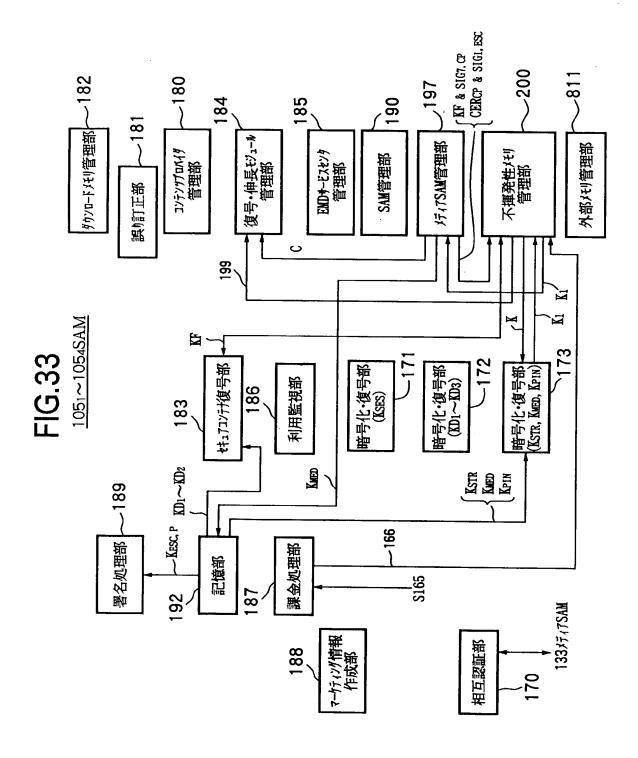


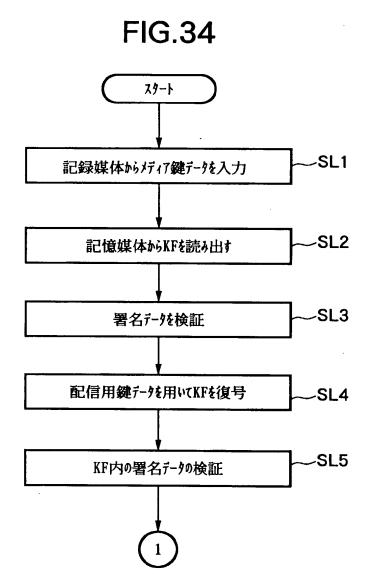
FIG.31



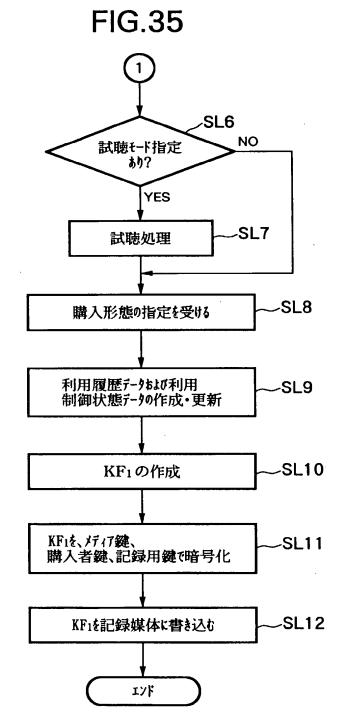
他のSAMから入力したCF等を記録媒体に書き込む際のSAMの処理







オンテインで配給されたコンテンツのSAMにおける購入形態決定処理



オフラインで配給されたコンテンツのSAMにおける購入形態決定処理

**FIG.36** 

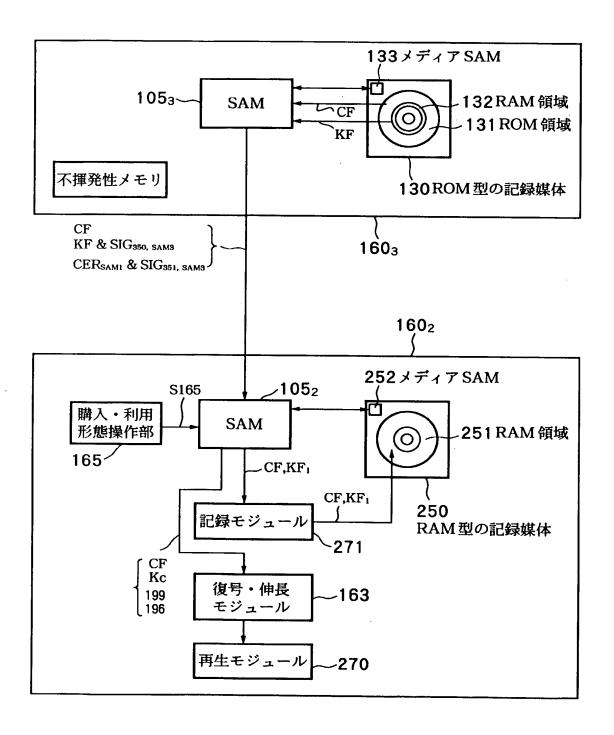
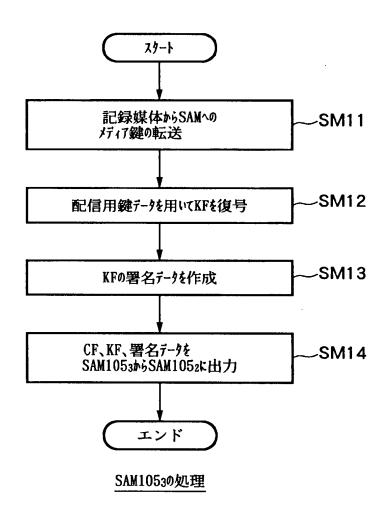


FIG.37



**FIG.38** 

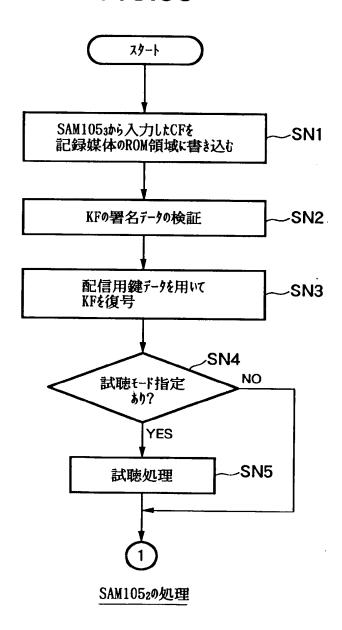
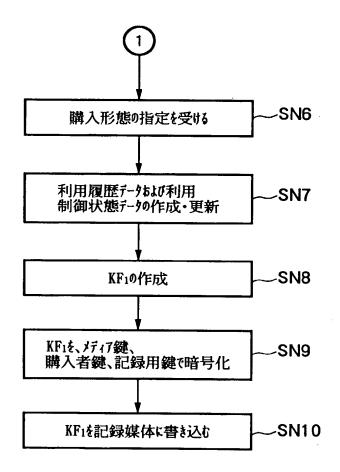
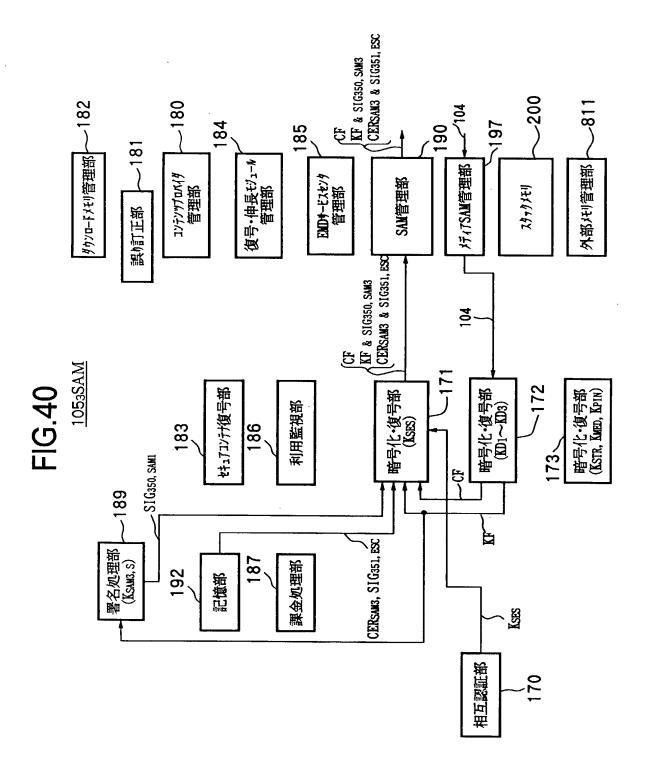
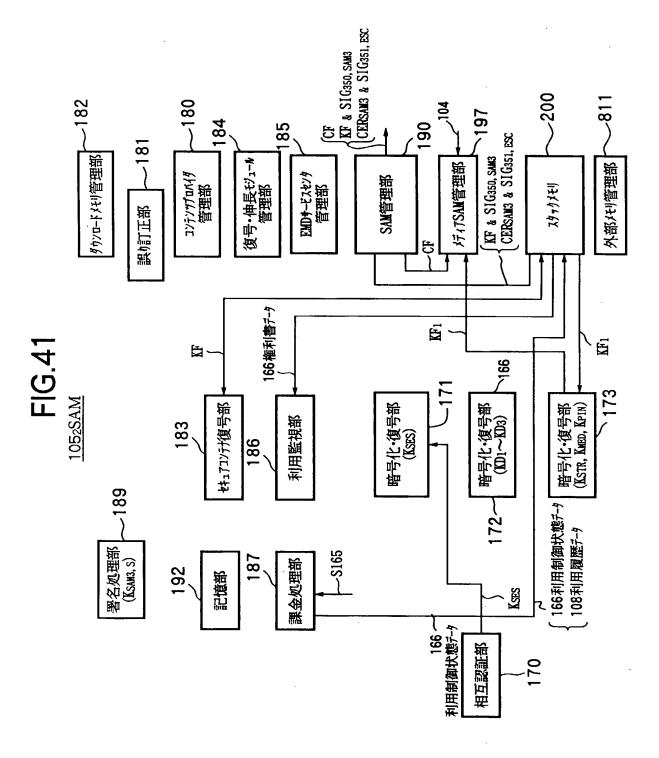


FIG.39



SAM10520処理





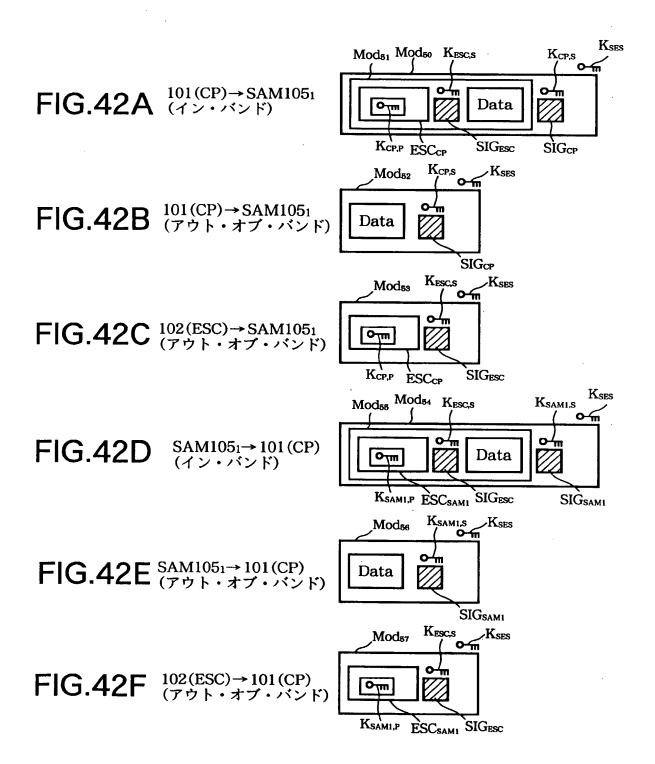


FIG.43A  $^{101(CP) \rightarrow 102(ESC)}_{(\checkmark \lor \cdot \lor \lor \lor)}$ 

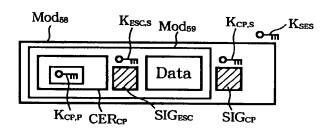


FIG.43B 101(CP)→102(ESC) (アウト・オブ・バンド)

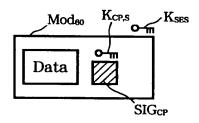


FIG.43C SAM1051→102(ESC)

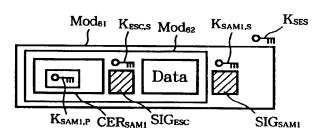


FIG.43D SAM1051→102(ESC) (アウト・オブ・バンド)

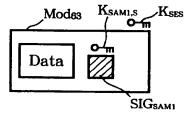
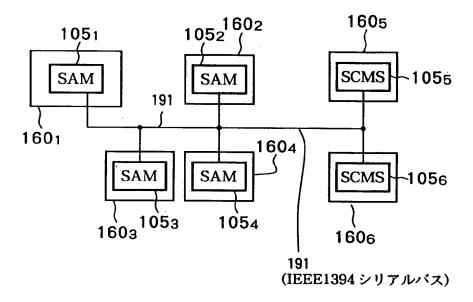


FIG.44



### **FIG.45**

リストを発行した SAM の SAM\_ID (Issure\_SAM)

SAM 登録リストの有効期限

SAM 登録数

SAM の接続リスト(SAM\_ID)

SAMの決済機能 有/無(Settlement Function)

Revocation\_Flag そのSAM がリボークされているか。

各々のSAMの公開鍵

ESC秘密鍵による署名データ

ハッシュ関数

リストを発行した SAM の SAM\_ID(Issure\_SAM)

Registration List の有効期限

SAM 登録数

SAMの接続リスト(SAM\_ID)

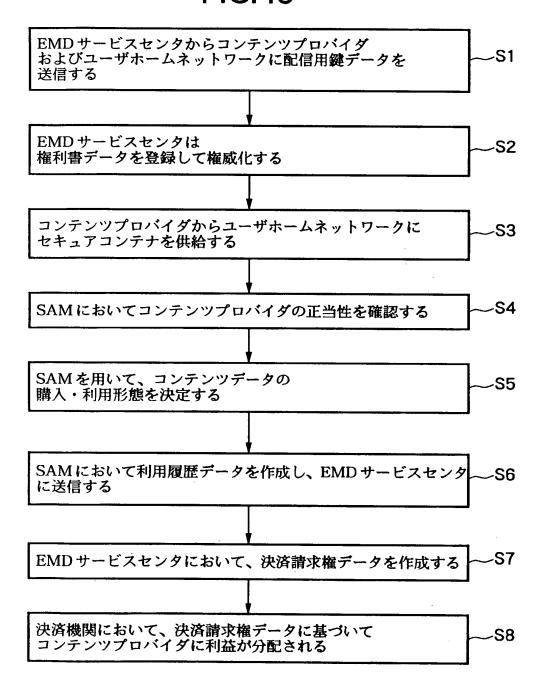
SAMの決済機能 有/無(Settlement Function)

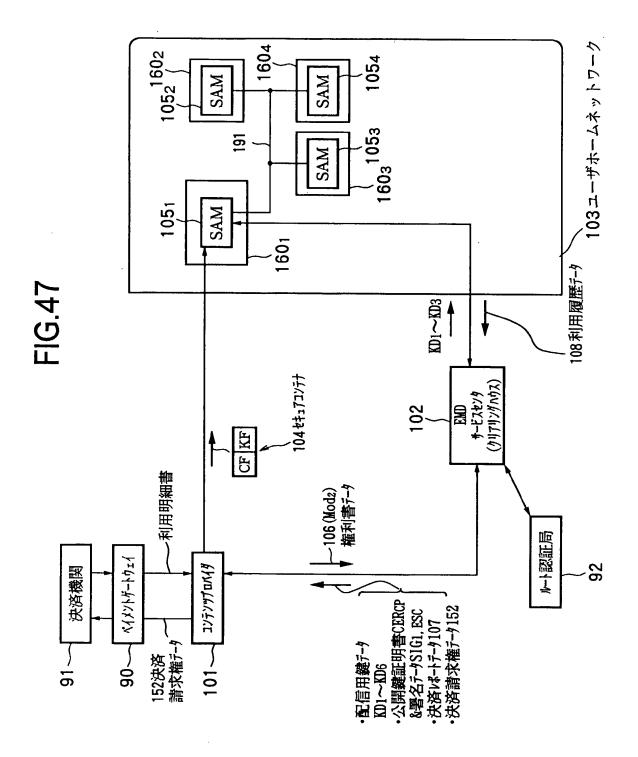
Revocation\_Flag そのSAM がリボークされているか。

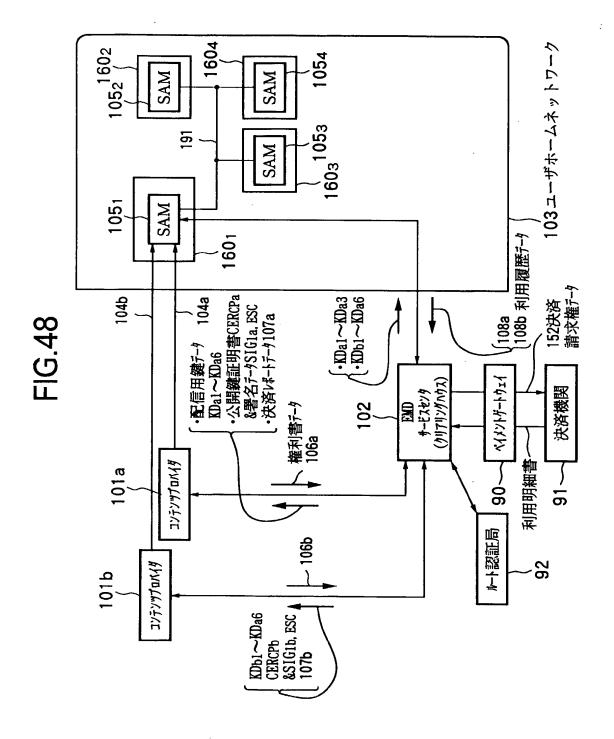
各々のSAMの公開鍵

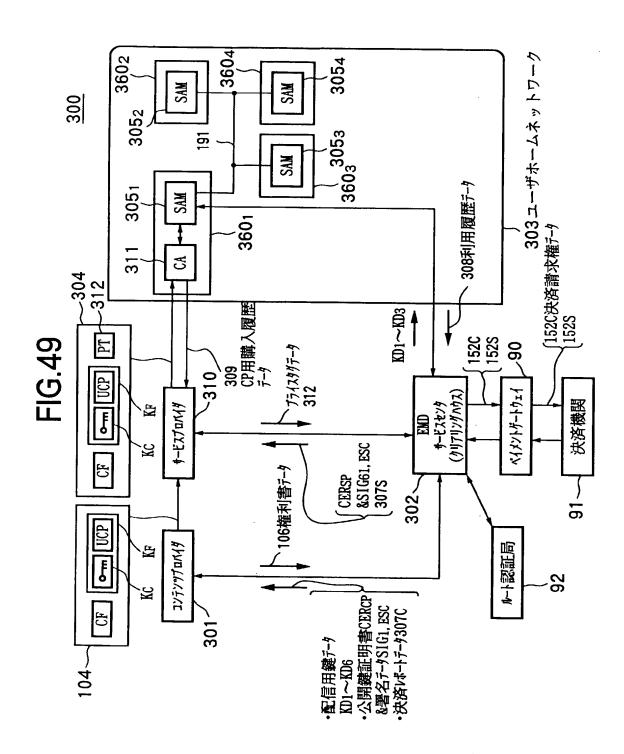
SAM登録リスト

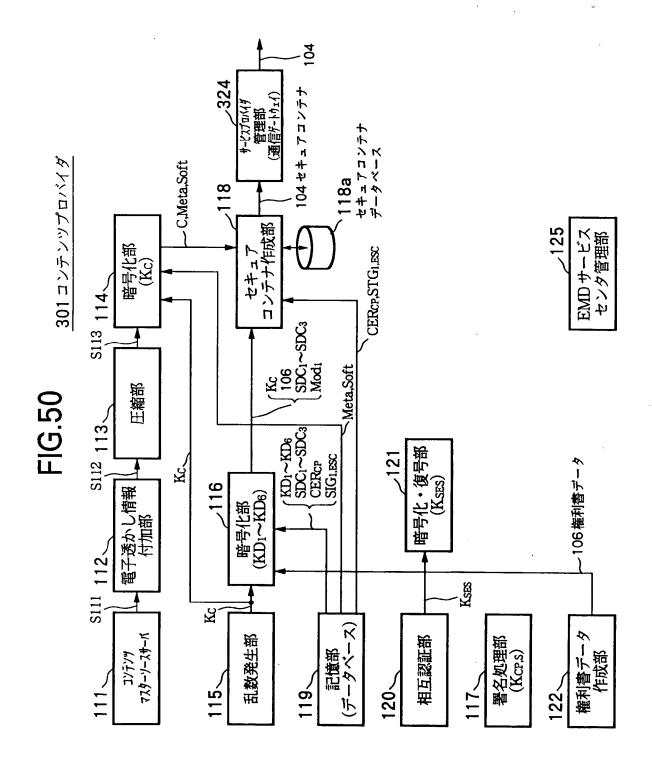
### **FIG.46**

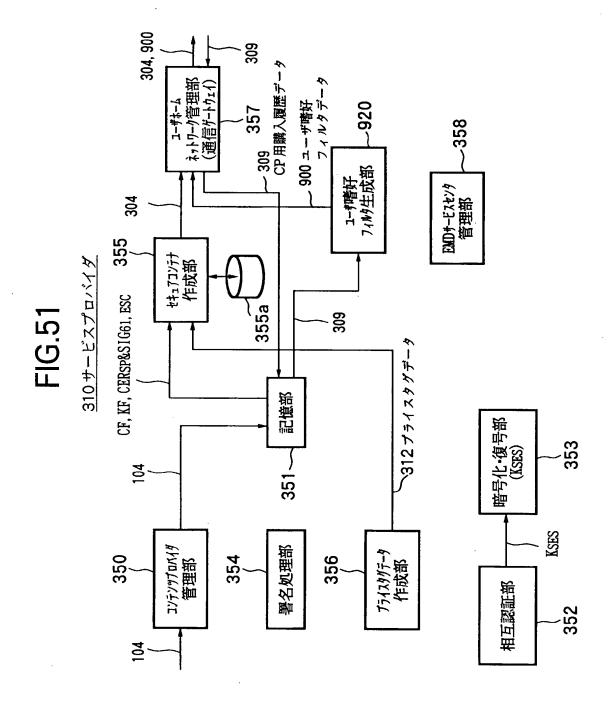




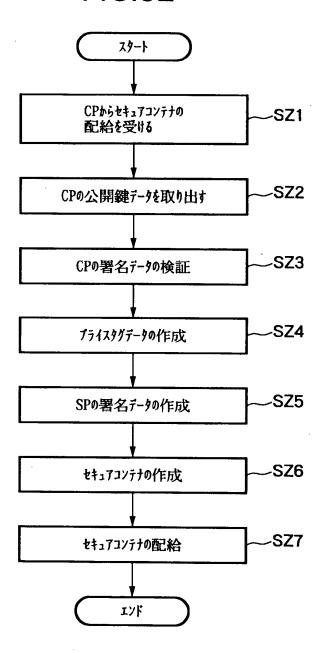


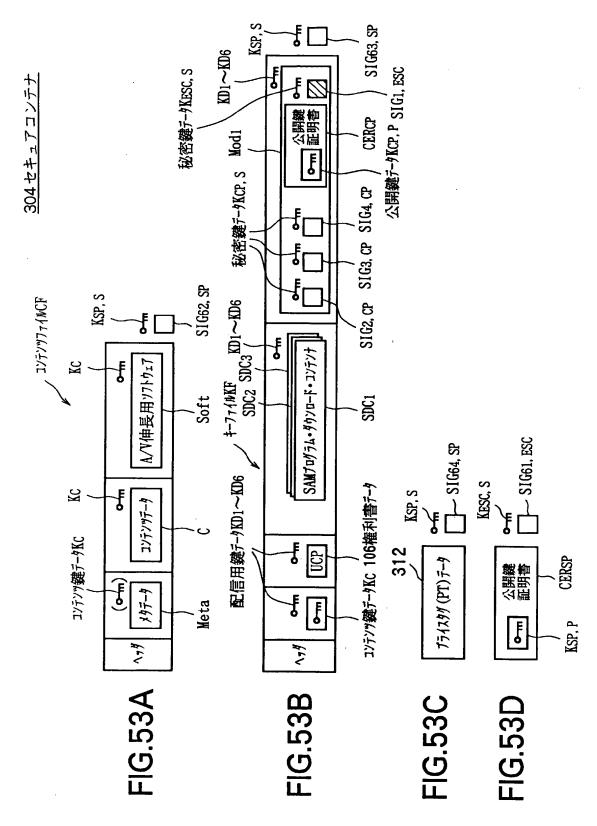






**FIG.52** 







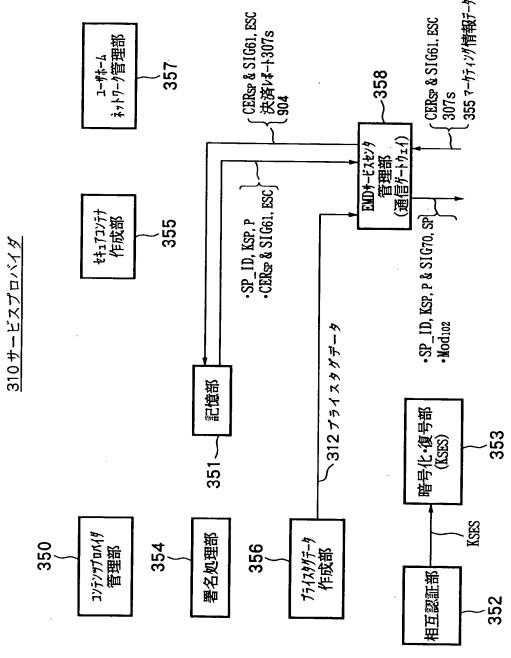


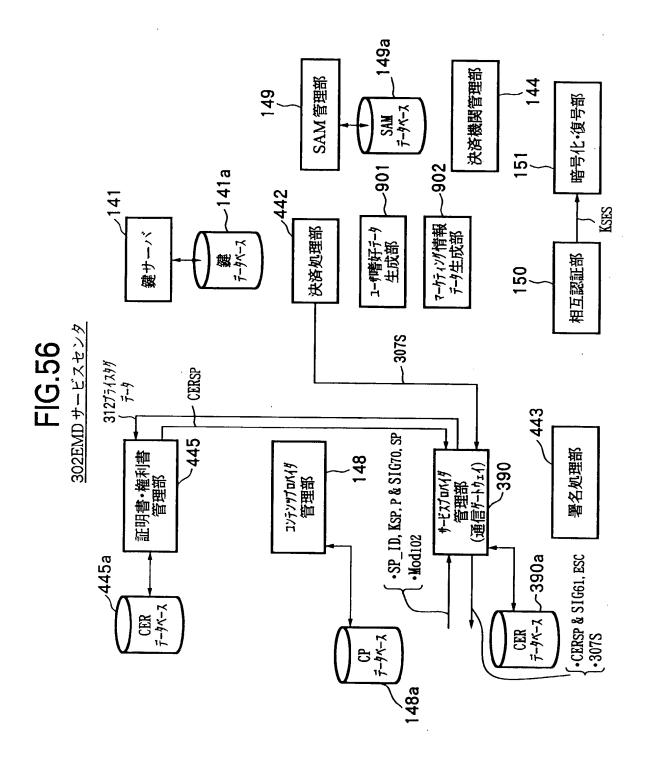
FIG.55

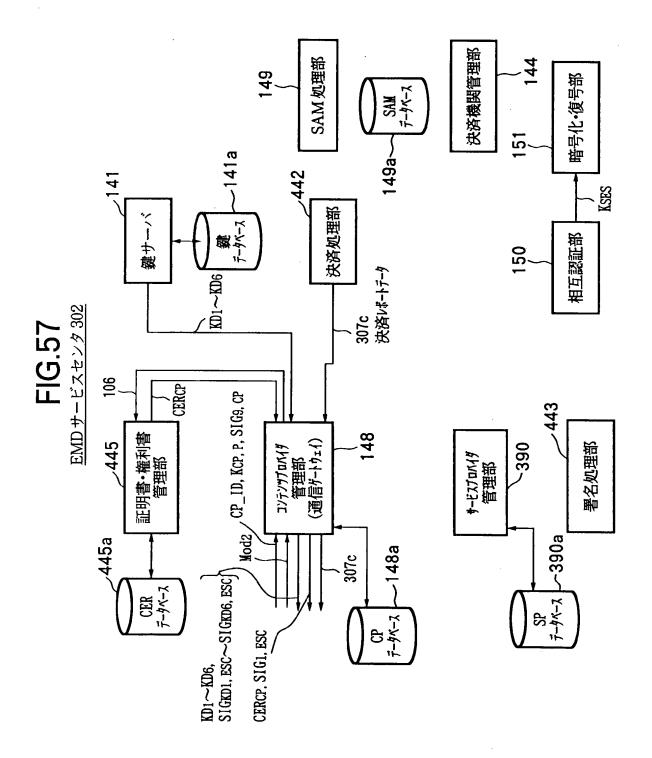
Modias プライスタゲ登録要求用モジュール

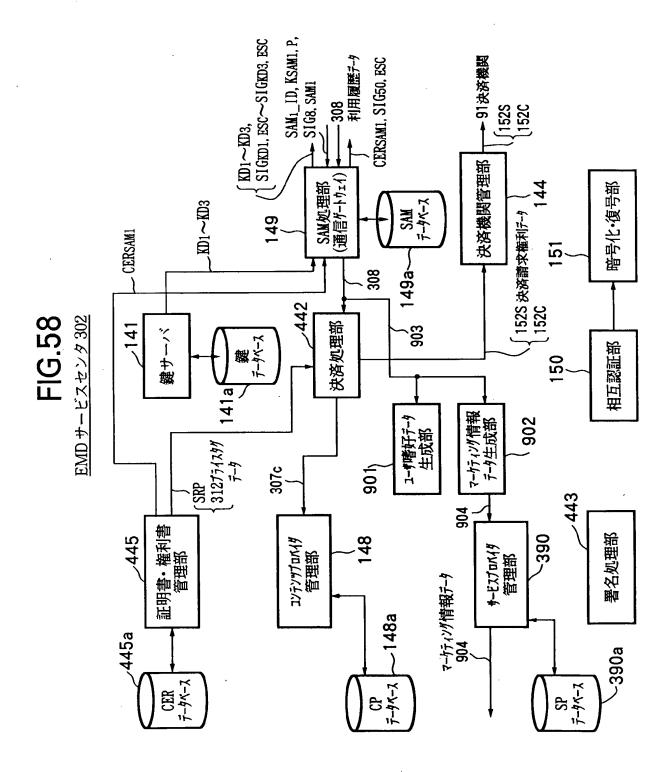
Modias アライスタゲ登録要求用モジュール

SP-ESC

Content\_D 106 SIG80.SP





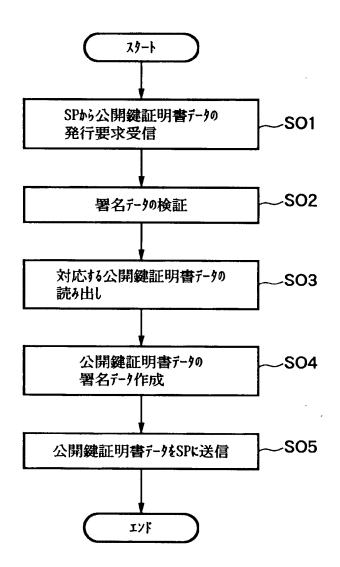


# FIG.59

### 利用履歴データ308の内容

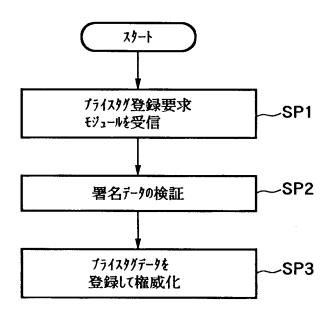
識別子 Content\_ID 識別子 CP\_ID 識別子 SP\_ID コンテンツデータ C の信号諸元データ コンテンツデータ C の圧縮方法 記録媒体の識別子 Media\_ID 識別子 SAM\_ID、 ユーザの USER\_ID

**FIG.60** 

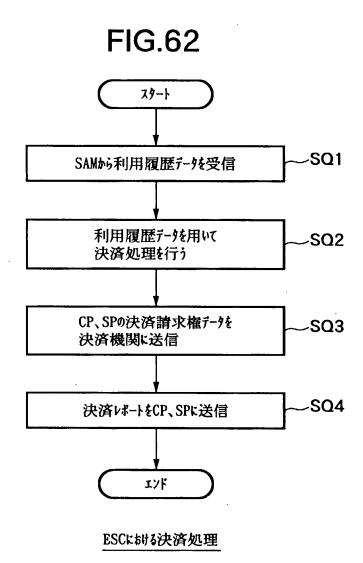


SPからの公開鍵証明書データの発行要求に応じたESCの処理

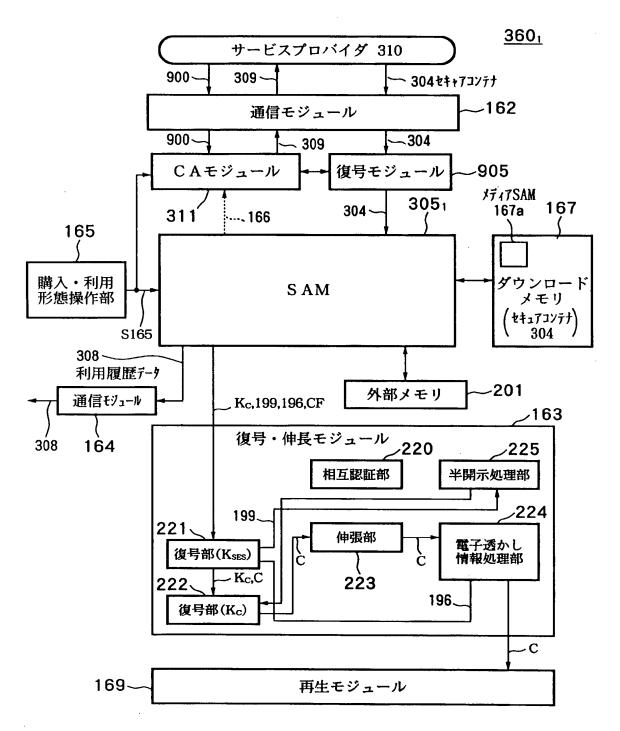
**FIG.61** 



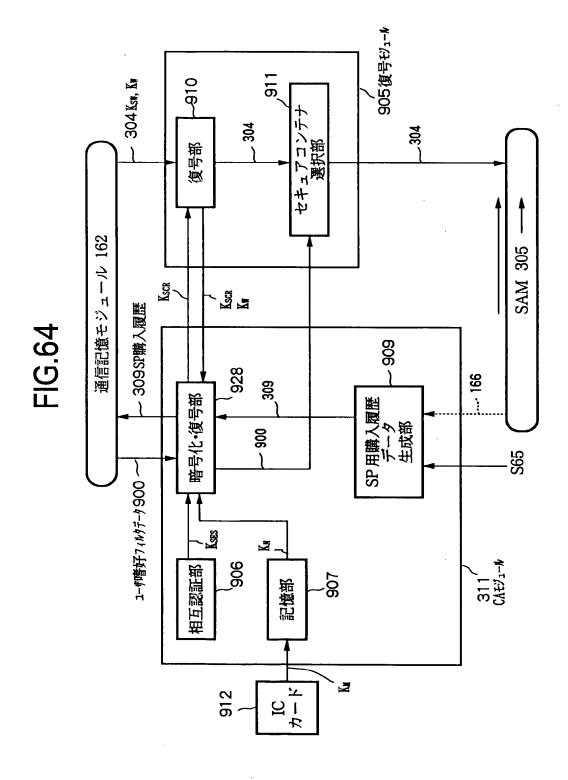
ESCにおけるブライスタグデータの登録処理

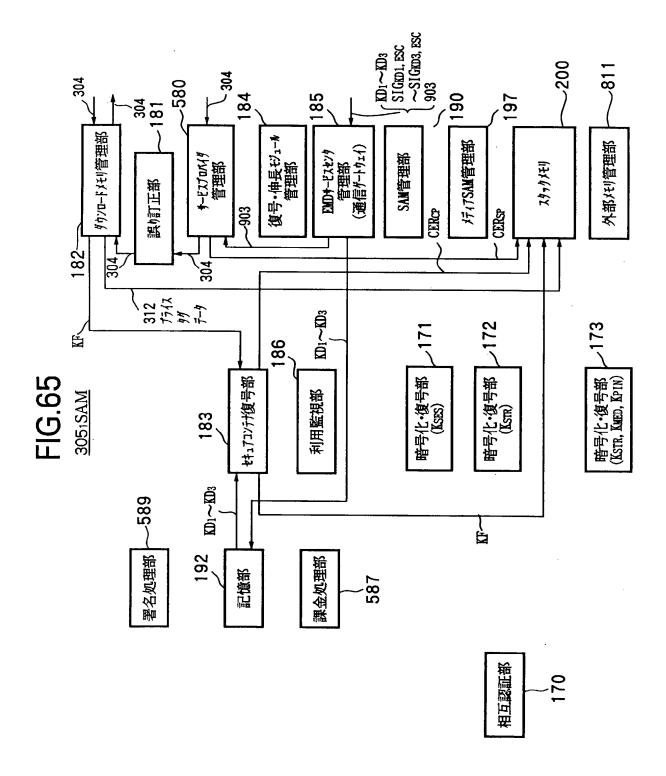


**FIG.63** 



61/99

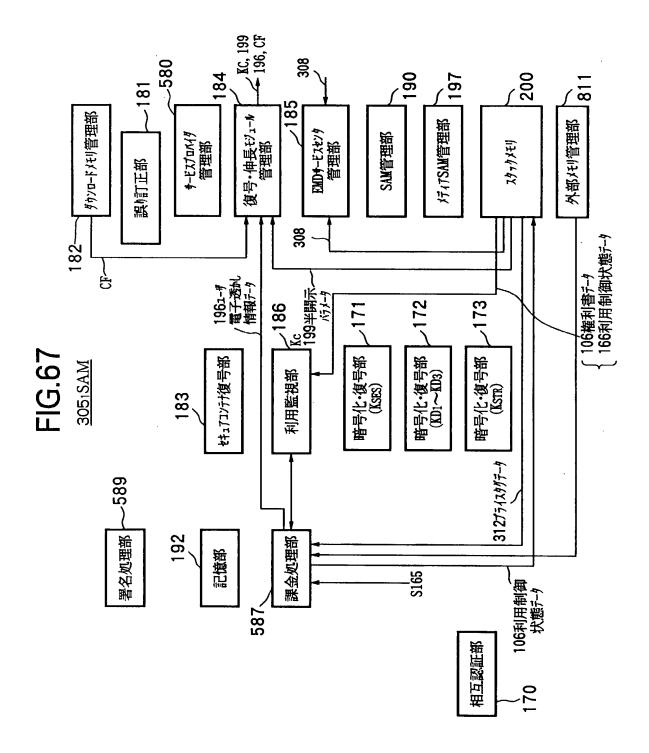




## FIG.66

### スタックメモリ 200 の記憶データ

コンテンツ鍵データ Kc 権利書データ (UCP) 106 不揮発性メモリ 201 のロック鍵データ K<sub>LOC</sub> コンテンツプロバイダ 301 の公開鍵証明書データ CER<sub>CP</sub> サービスプロバイダ 301 の公開鍵証明書データ CER<sub>SP</sub> 利用制御情状態データ (UCS) 166 SAM プログラム・ダウンロード・コンテナ SD<sub>1</sub>~SDC<sub>3</sub> プライスタグデータ 312



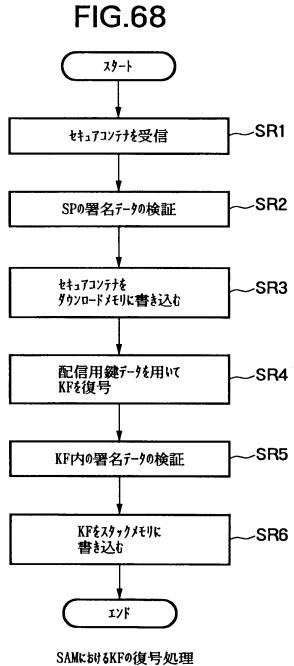
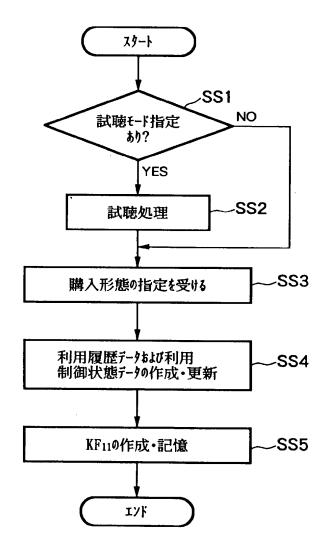
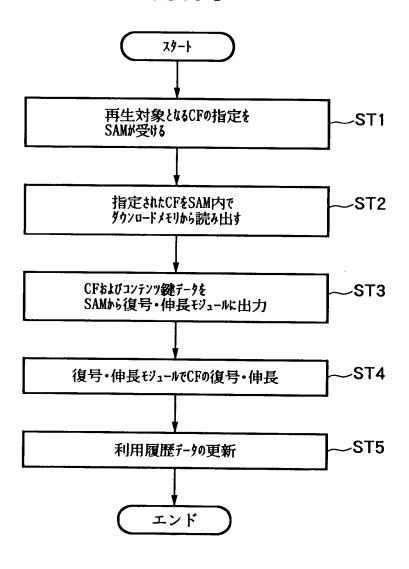


FIG.69



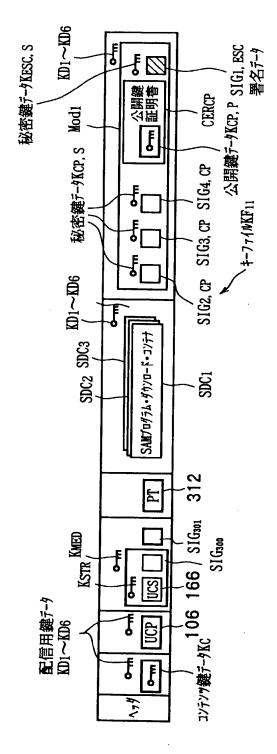
SAMにおけるセキュアコンテナの購入形態決定処理

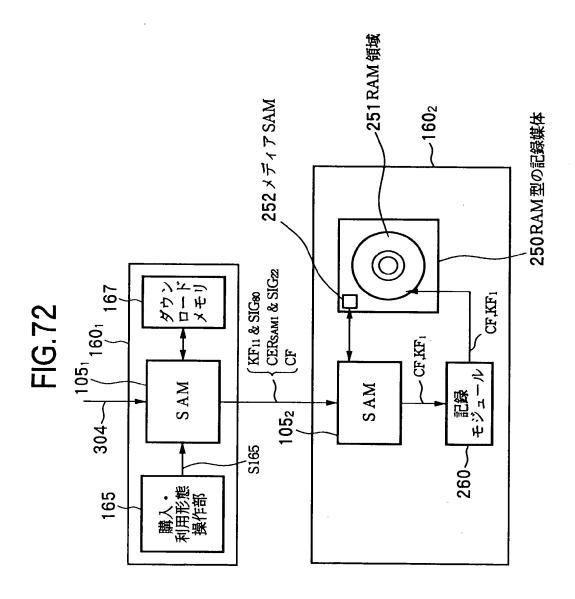


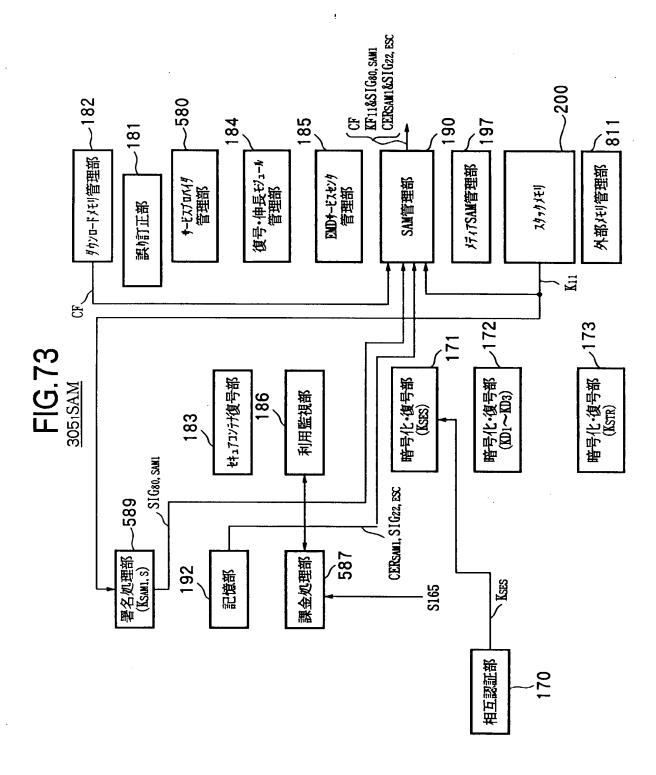


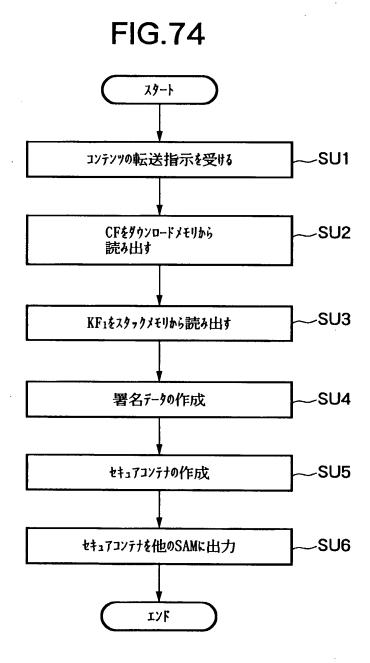
コンテンツデータの再生処理

FIG. 71

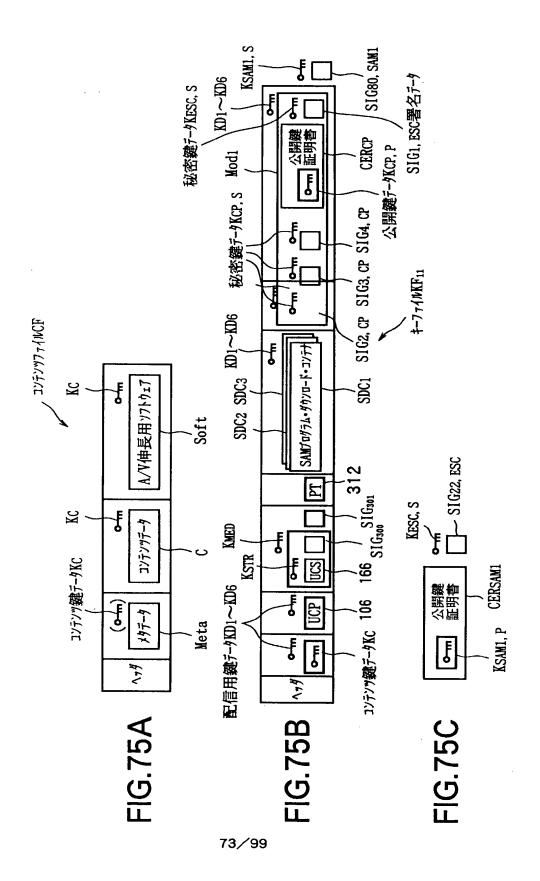


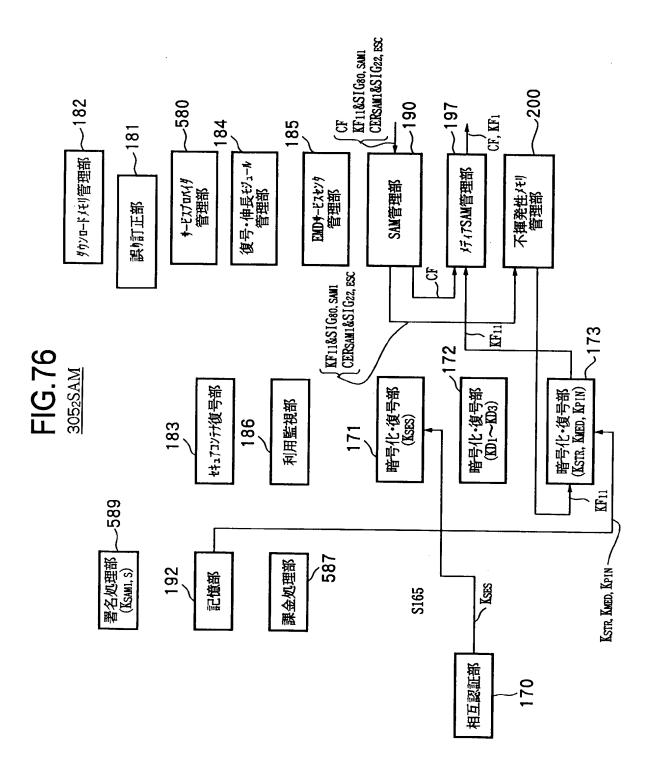




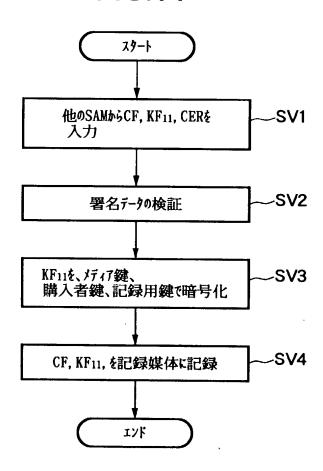


購入形態決定後のコンテンツを他のSAMに転送するSAMの処理





**FIG.77** 



他のSAMから入力したCF等を記録媒体に書き込む際のSAMの処理

### **FIG.78**

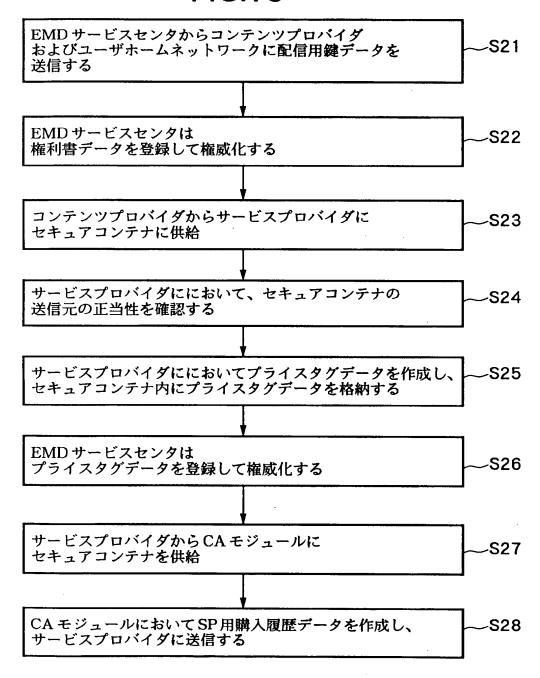
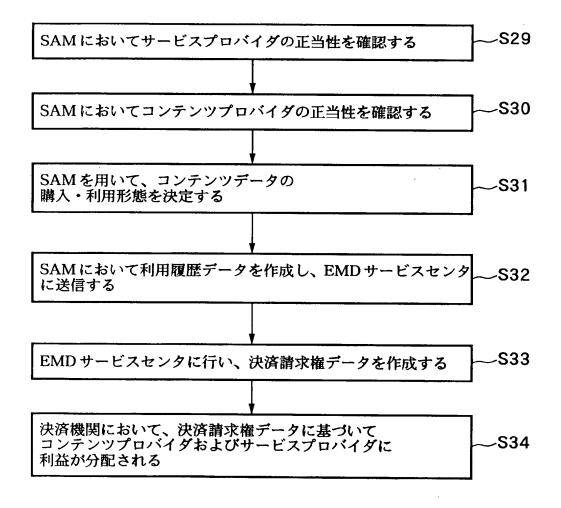
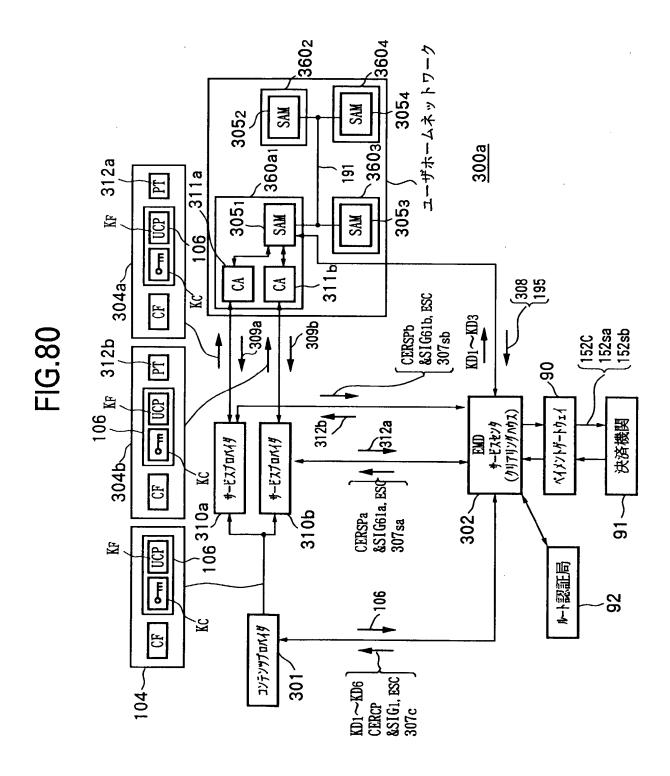
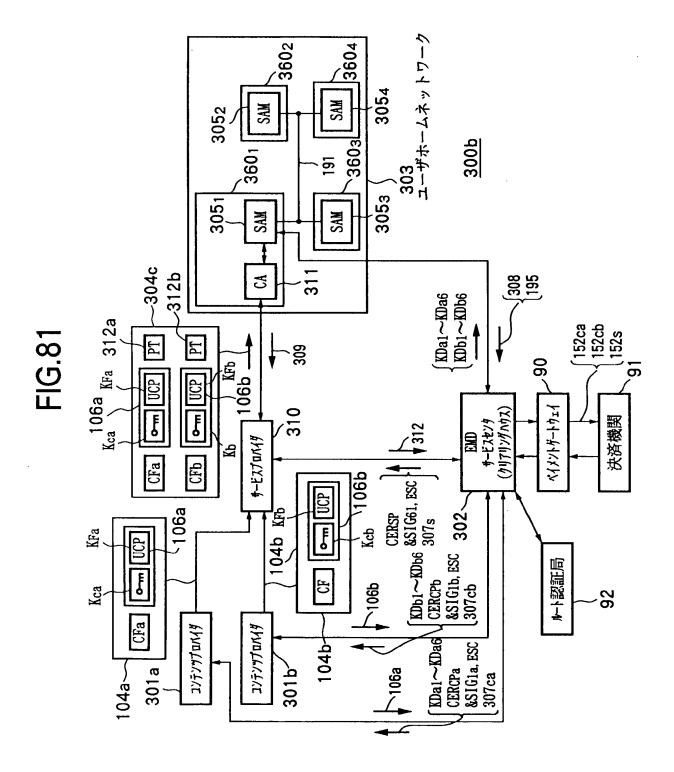


FIG.79

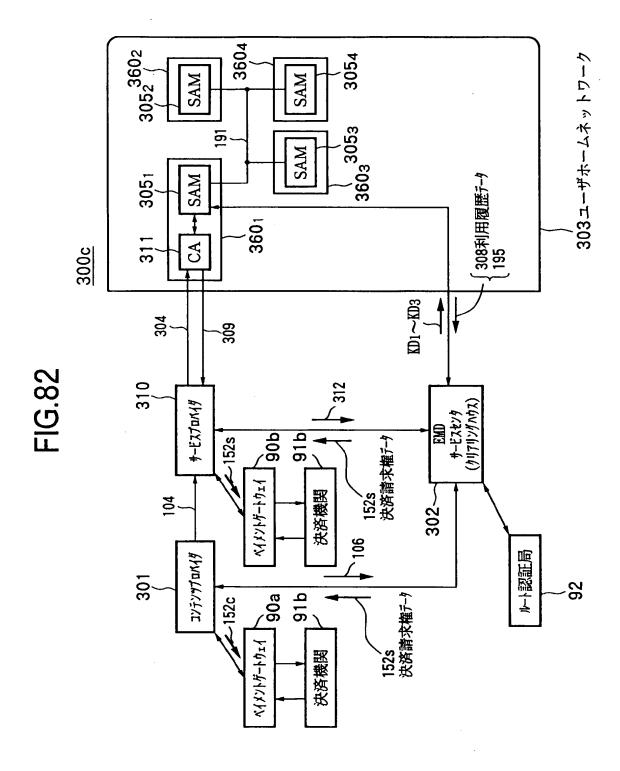


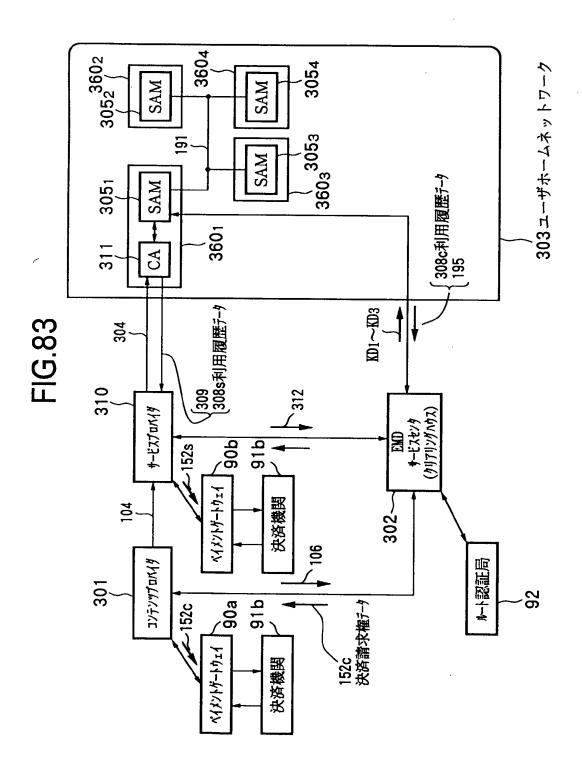


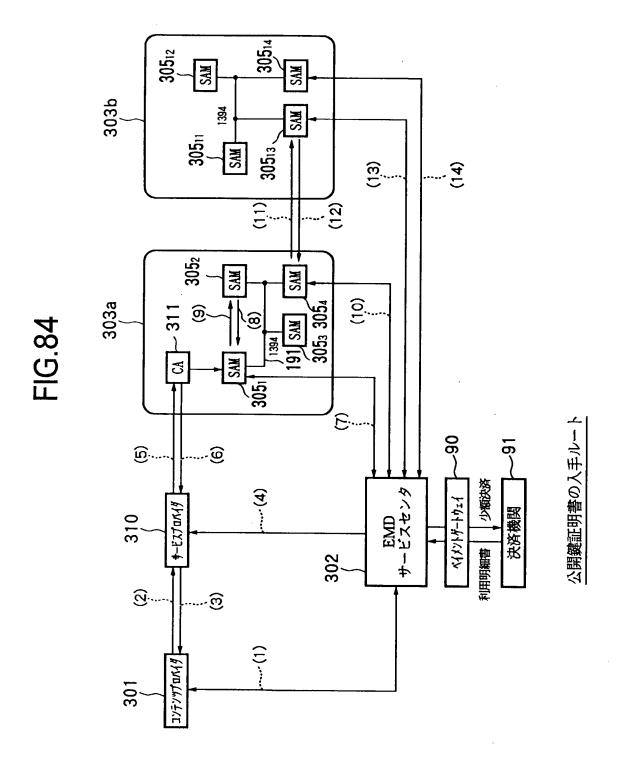
78/99

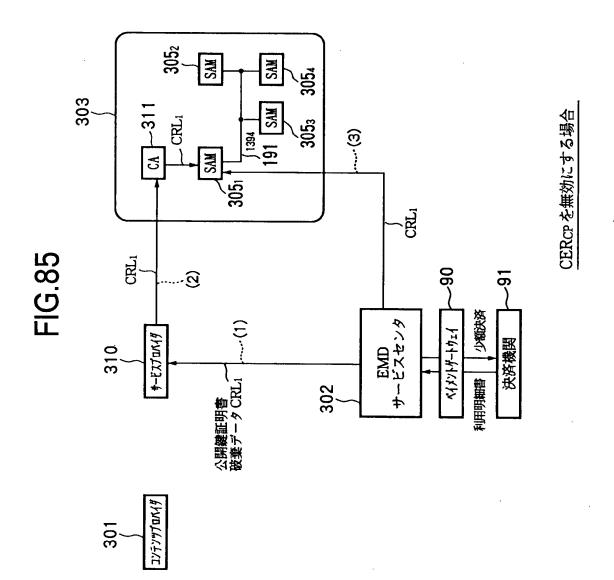


79/99

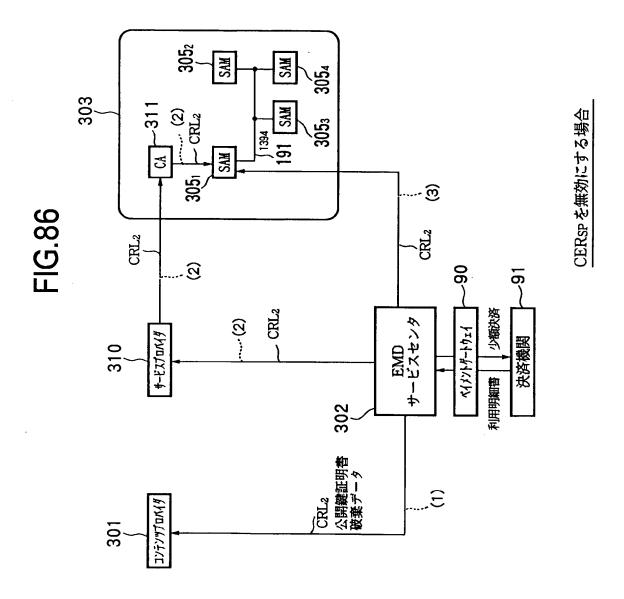




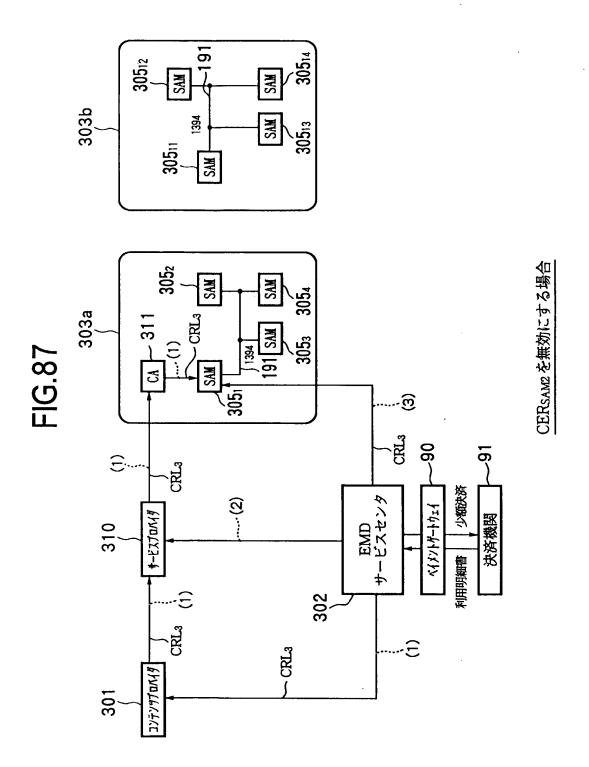


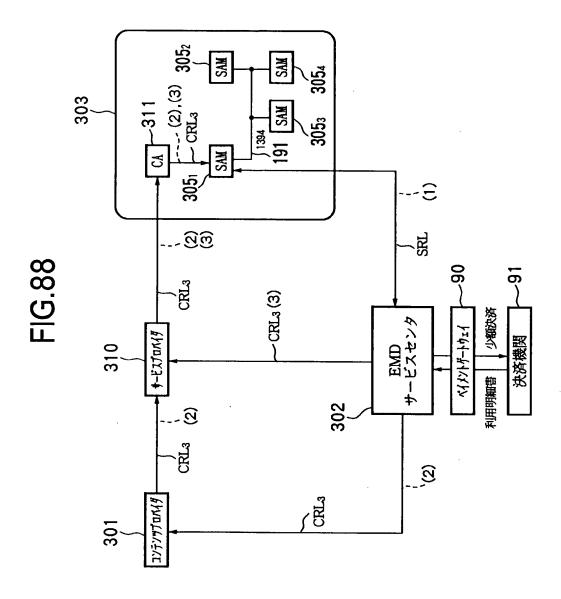


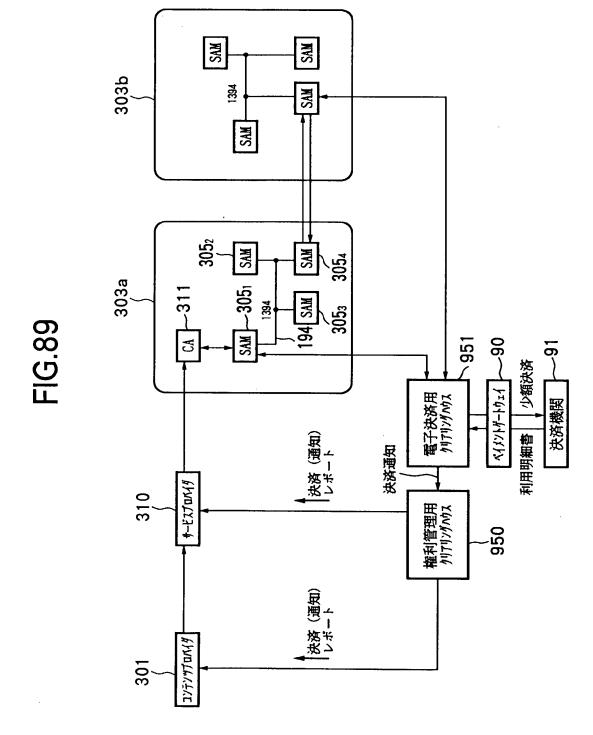
83/99

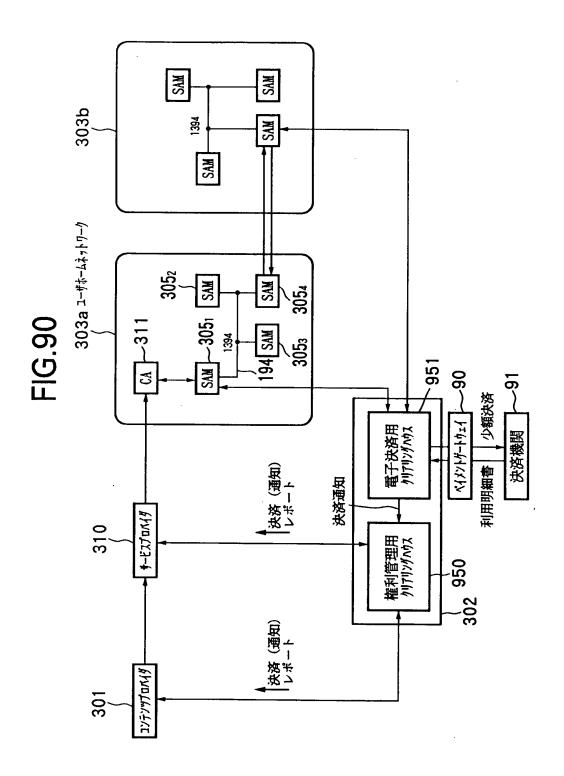


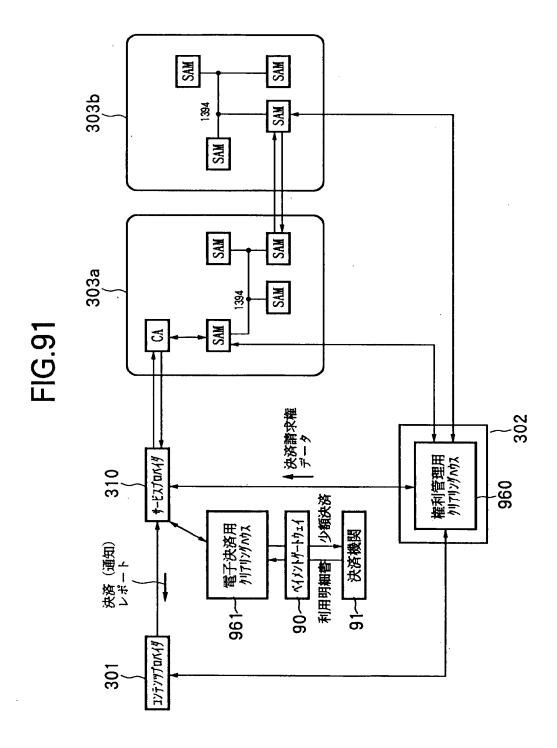
84/99

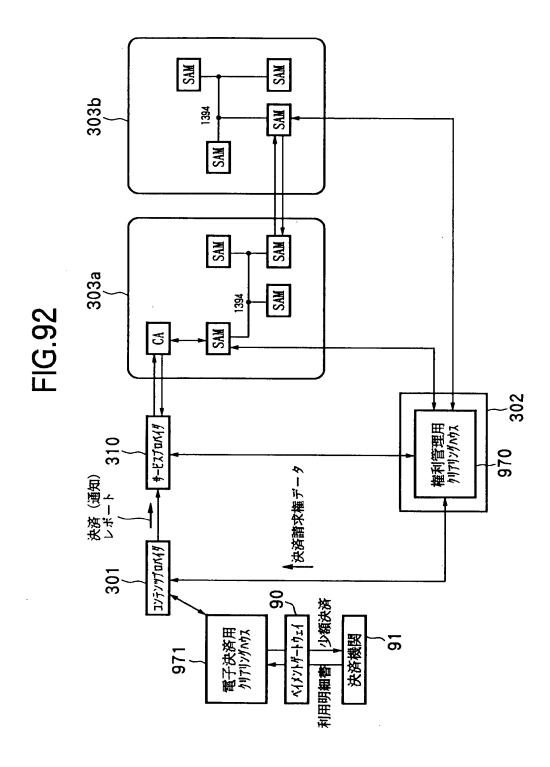


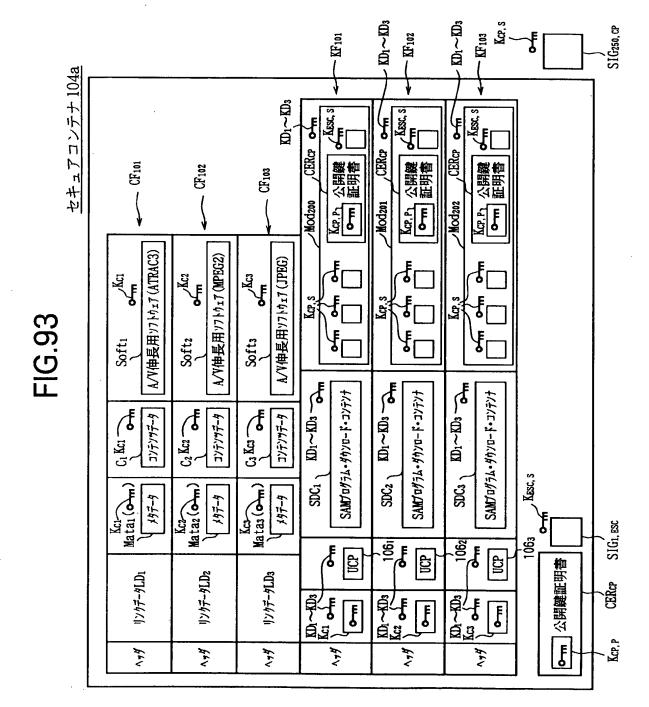












91/99

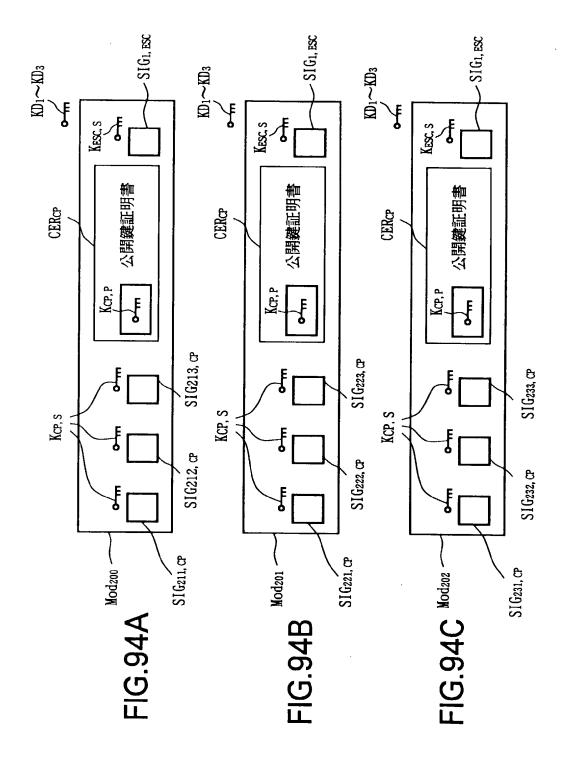
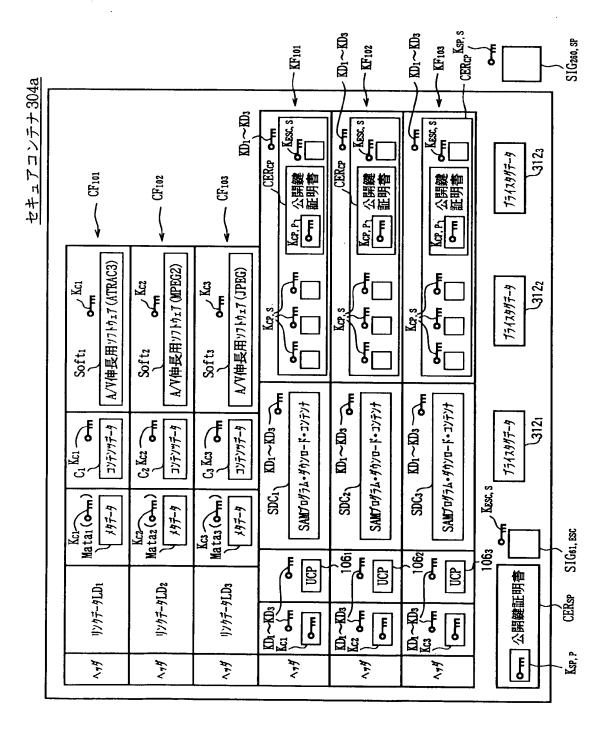
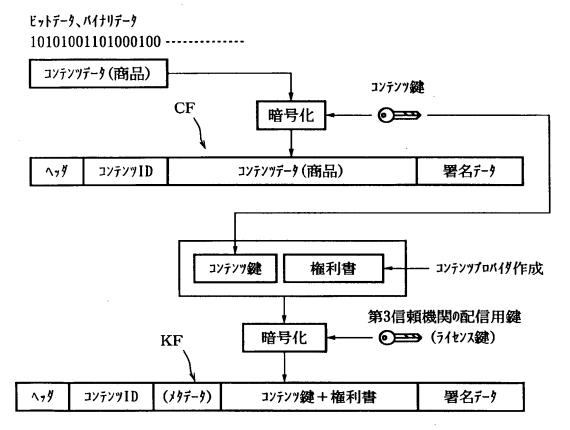


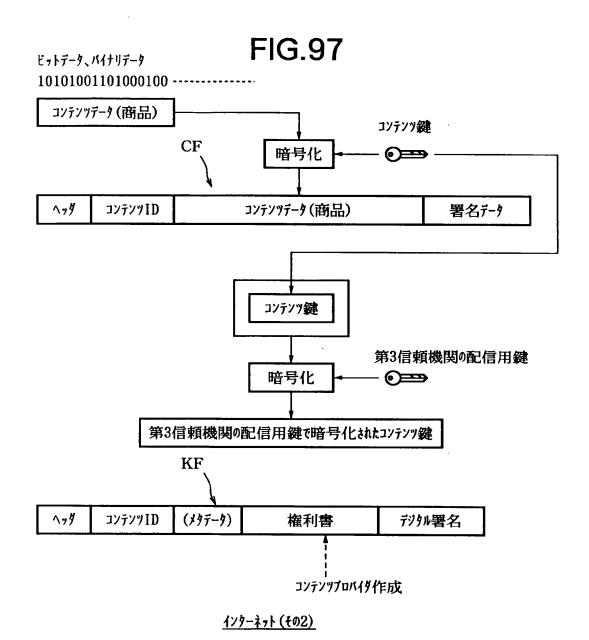
FIG.95



**FIG.96** 

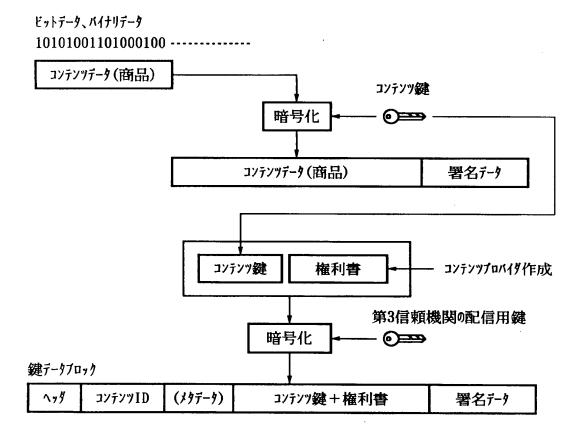


<u>インターネット (その1)</u>



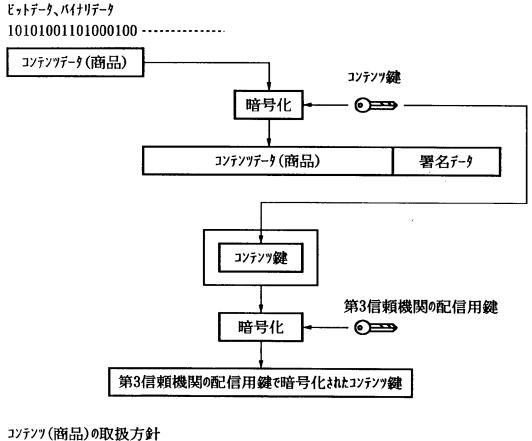
95/99

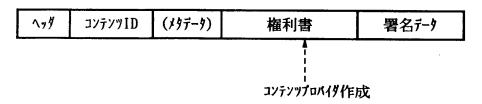
# **FIG.98**



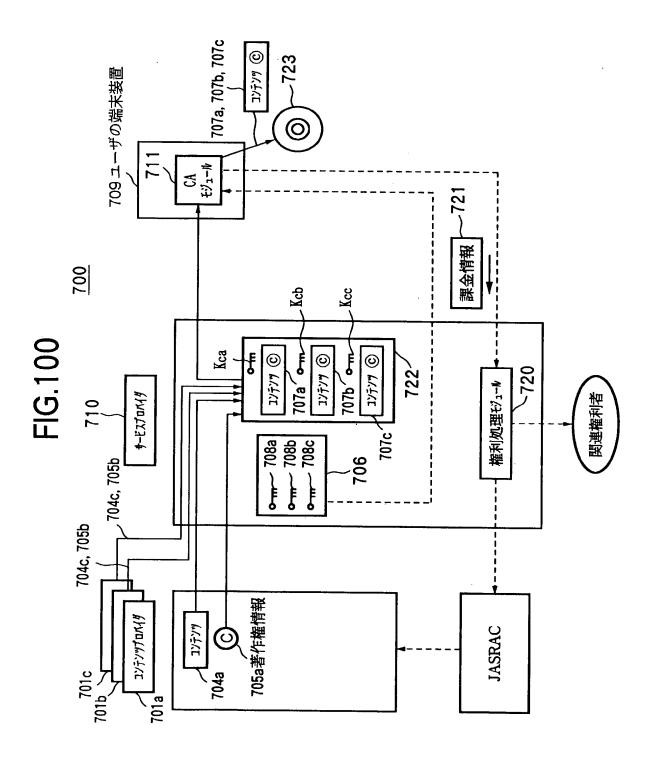
テシタル放送(その1)

**FIG.99** 





デジタル放送(その2)



## 符号リスト

- 90…ペイメントゲートウェイ
- 9 1 …決済機関
- 9 2 …ルート認証局
- 100, 300…EMDシステム
- 101,301…コンテンツプロバイダ
- 102, 302…EMDサービスセンタ
- 103, 303…ユーザホームネットワーク
- 104, 304…セキュアコンテナ
- $105_1 \sim 105_4$ ,  $305_1 \sim 305_4$  ... SAM
- 106…権利書データ
- 107,307…決済レポートデータ
- 108,308…利用履歴データ
- 1601 …ネットワーク機器
- 1602~1604····AV機器
- 152, 152c, 152s…決済請求権データ
- 191…バス
- 310…サービスプロバイダ
- 311…CAモジュール
- 312…プライスタグデータ
- CF・・・コンテンツファイル
- KF·・・・キーファイル
- K c…コンテンツ鍵データ

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/04488

A.	CLASS Int.	SIFICATION OF SUBJECT MATTER .Cl <sup>7</sup> G06F15/00, G06F17/60, H041	L9/08, H04L9/32, G10K15/	02, G06F13/00	
Acc	ording t	to International Patent Classification (IPC) or to both n	ational classification and IPC		
		S SEARCHED			
Min	imum do Int.	ocumentation searched (classification system followed . Cl <sup>7</sup> G06F15/00, G06F17/60, H041	by classification symbols) L9/08, H04L9/32, G10K15/	02, G06F13/00	
	Jits Koka	tion searched other than minimum documentation to the suyo Shinan Koho 1926-1996 ai Jitsuyo Shinan Koho 1971-2000	Jitsuyo Shinan Toroku R Toroku Jitsuyo Shinan R	Koho 1996-2000 Koho 1994-2000	
Elec	CS D	lata base consulted during the international search (name DATABASE, WPI, JICST SCIENCE and cribution, SuperDistribution	ne of data base and, where practicable, sea TECHNOLOGY DOCUMENT DATA	urch terms used) ABASE contents,	
C.	DOCUI	MENTS CONSIDERED TO BE RELEVANT			
Cate	egory*	Citation of document, with indication, where ap	ppropriate, of the relevant passages	Relevant to claim No.	
	Х	WO, 96/27155, A3 (Electronic Publ 06 September, 1996 (06.09.96), pages 165 to 177, 386 to 412, 9 & JP, 10-512074, W & AU, 9663 & EP, 861461, A2 & US, 5910	597 to 602, 638 to 644 266, A 987, A	1-14,16-36, 38-71,142, 150-171, 183-204	
	Y	& US, 5915019, A & US, 5917 & US, 5949876, A & US, 5982	912, A 891, A	15,37,99-108, 110-115, 117-136, 138-141, 175-182,208	
	А			72-98,109,116, 137,143-149, 172-174, 205-207	
	Y	WO, 98/10381, A1 (Intertrust Te 12 March, 1998 (12.03.98), pages 104 to 142, 168 to 190		15, 37, 99-108, 110-115, 117-136, 138-141, 175-182,208	
$\boxtimes$	Further	r documents are listed in the continuation of Box C.	See patent family annex.		
"A" "E" "L" "O" "P"	Special categories of cited documents: document defining the general state of the art which is not considered to be of particular relevance earlier document but published on or after the international filing date document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) document referring to an oral disclosure, use, exhibition or other means document published prior to the international filing date but later than the priority date claimed of the actual completion of the international search		"T" later document published after the inte priority date and not in conflict with th understand the principle or theory understand the considered novel or cannot be considered to involve an inventive step combined with one or more other such combination being obvious to a person document member of the same patent for the same patent for the same patent for mailing of the international search.	n the application but cited to inderlying the invention he claimed invention cannot be dered to involve an inventive one he claimed invention cannot be step when the document is such documents, such son skilled in the art in family	
Name		ovember, 2000 (14.11.00) ailing address of the ISA/	21 November, 2000 (2  Authorized officer	:1.11.00)	
Japanese Patent Office					
Facsimile No.		).	Telephone No.		

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/04488

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No
A	JP, 11-85504, A (Mitsubishi Electric Corporation), 30 March, 1999 (30.03.99), See the full text (Family: none)	1-208
A	See the full text (Family: none)  JP, 10-161937, A (Toshiba Corporation), 19 June, 1998 (19.06.98), See the full text (Family: none)	1-208

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

### INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/04488

	Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)
This inte	ernational search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:
. 🗂	Claima Nea :
1.	Claims Nos.: because they relate to subject matter not required to be searched by this Authority, namely:
	occurse in the second subject manner is a second subject to the se
2.	Claims Nos.:
2.	because they relate to parts of the international application that do not comply with the prescribed requirements to such an
	extent that no meaningful international search can be carried out, specifically:
3.	Claims Nos.: because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).
	Observations where unity of invention is lacking (Continuation of item 2 of first sheet)
This Inte	ernational Searching Authority found multiple inventions in this international application, as follows:
	The inventions of the international application are separated into 14 groups:
96 CT	aims 1-71/ claims 72-76, 79-81, 83-89, 92-95, 97/ claims 77, 78, 82, 90, 91, 98/ claims 99-141, 180-182/ claims 142-149/150, 183/ claims 151, 152, 184,
1.8	5/ claims 153, 154, 186, 187/ claims 155-157, 160-165, 188-190, 193-198/ claims
	8, 191/ claims 159, 192/ claims 166-171, 199-204/ claims 172-174, 205-207/
and	d claims 175-179, 208.
1.	As all required additional search fees were timely paid by the applicant, this international search report covers all searchable
	claims.
2.	As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment
	of any additional fee.
3.	As only some of the required additional search fees were timely paid by the applicant, this international search report covers
"   _	only those claims for which fees were paid, specifically claims Nos.:
İ	
l _	
4.	No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
	search report is restricted to the invention first mentioned in the claims, it is covered by claims 190s
Remar	k on Protest  The additional search fees were accompanied by the applicant's protest.
	No protest accompanied the payment of additional search fees.

#### A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. C1' G06F15/00, G06F17/60, H04L9/08, H04L9/32, G10K15/02, G06F13/00

#### B. 調査を行った分野

調査を行った最小限資料(国際特許分類(IPC))

Int. Cl<sup>7</sup> G06F15/00, G06F17/60, H04L9/08, H04L9/32, G10K15/02, G06F13/00

#### 最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報

1926-1996年

日本国公開実用新案公報

1971-2000年

日本国実用新案登録公報

1996-2000年

日本国登録実用新案公報

1994-2000年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

CSデータベース,WPI,JICST科学技術文献データベース contents, distribution, SuperDistribution

#### C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	WO, 96/27155, A3 (Electronic Publishing Resources, Inc.) 6.9月.1996(06.09.96), 第165-177, 386-412, 597-602, 638-644頁	1-14, 16-36, 3 8-71, 142, 150 -171, 183-204
Y	& JP, 10-512074, W & AU, 9663266, A & EP, 861461, A2 & US, 5910987, A & US, 5915019, A & US, 5917912, A & US, 5949876, A & US, 5982891, A	15, 37, 99– 108, 110–115, 117–136, 138– 141, 175–182, 208

#### 区欄の続きにも文献が列挙されている。

□ パテントファミリーに関する別紙を参照。

#### \* 引用文献のカテゴリー

- 「A」特に関連のある文献ではなく、一般的技術水準を示す もの
- 「E」国際出願日前の出願または特許であるが、国際出願日 以後に公表されたもの
- 「L」優先権主張に疑義を提起する文献又は他の文献の発行 日若しくは他の特別な理由を確立するために引用する 文献(理由を付す)
- 「〇」口頭による開示、使用、展示等に言及する文献
- 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

- の日の後に公表された文献
- 「T」国際出願日又は優先日後に公表された文献であって 出願と矛盾するものではなく、発明の原理又は理論 の理解のために引用するもの
- 「X」特に関連のある文献であって、当該文献のみで発明 の新規性又は進歩性がないと考えられるもの
- 「Y」特に関連のある文献であって、当該文献と他の1以 上の文献との、当業者にとって自明である組合せに よって進歩性がないと考えられるもの
- 「&」同一パテントファミリー文献

C (続き) .	関連すると認められる文献	
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A		72-98, 109, 116, 137, 143- 149, 172-174, 205-207
Y	WO, 98/10381, A1 (Intertrust Technologies Corp.) 12. 3月.1998(12.03.98), 第104-142, 168-190頁(ファミリなし)	15, 37, 99– 108, 110–115, 117–136, 138– 141, 175–182, 208
A	JP, 11-85504, A (三菱電機株式会社) 30. 3月.1999(30.03.99), 全頁を参照 (ファミリなし)	1-208
A	JP, 10-161937, A (株式会社東芝) 19. 6月.1998(19.06.98), 全頁を参照 (ファミリなし)	1-208

第I欄	請求の範囲の一部の調査ができないときの意見(第1ページの2の続き)			
法第8条第3項(PCT17条(2)(a))の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。				
1.	請求の範囲は、この国際調査機関が調査をすることを要しない対象に係るものである。 つまり、			
2.	請求の範囲 は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、			
	。			
з. П	請求の範囲 は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に			
3.	請求の範囲は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に 従って記載されていない。			
第Ⅱ欄	発明の単一性が欠如しているときの意見 (第1ページの3の続き)			
次に过	べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。			
/99- -190	の出願の発明は、請求の範囲1-71/72-76, 79-81, 83-89, 92-95, 97/77, 78, 82, 90, 91, 96, 98/-141, 180-182/142-149/150, 183/151, 152, 184, 185/153, 154, 186, 187/155-157, 160-165, 188 0, 193-198/158, 191/159, 192/166-171, 199-204/172-174, 205-207/175-179, 208の 1 4 群の			
発明	に区分される。			
1. X	出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求 の範囲について作成した。			
2.	追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追 加調査手数料の納付を求めなかった。			
3. 🗌	出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。			
4.	出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。			
追加調査	三手数料の異議の申立てに関する注意 ] 追加調査手数料の納付と共に出願人から異議申立てがあった。			
K	追加調査手数料の納付と共に出願人から異議申立てがなかった。			